Leiden University

ICT in Business and the Public Sector

Lowering the Barriers: A Best-Practice Approach to Cyber Supply Chain Risk Management.

Name:	Camiel Oscar van Schaik
Student ID:	s2520753
Date:	June 25, 2025
1st supervisor:	Prof.dr.ir. J.M.W. Visser
2nd supervisor:	Dr.ir. E. Makri MSc
Company supervisor:	M. Solen

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)
Leiden University
Einsteinweg 55
2333 CC Leiden
The Netherlands

Abstract

Background: As digital transformation accelerates and supply chains grow increasingly complex and interdependent, organizations are becoming more vulnerable to cyber threats introduced through suppliers. Despite the existence of various standards and frameworks from institutions like NIST and ISO, the Cyber Supply Chain Risk Management (C-SCRM) landscape remains fragmented and difficult to navigate, particularly for small and mid-sized enterprises facing a knowledge shortage in this domain. The growing regulatory demands, such as those posed by the EU's NIS2 Directive, add further pressure on organizations to implement comprehensive risk management strategies. However, the lack of accessible and actionable implementation guidance hampers effective adoption in these types of organizations.

Aim: This research aims to develop a practical and accessible best practices implementation guideline for Cyber Supply Chain Risk Management (C-SCRM). The guideline is designed to consolidate existing academic insights, industry standards, and expert perspectives into a coherent step-by-step approach that supports organizations, especially those with limited cybersecurity expertise, in enhancing their supply chain security. A key objective is to evaluate the extent to which this guideline aligns with and supports compliance with NIS2 Article 21.2.d.

Method: The research follows a three-cycle methodology. First, a comprehensive literature review is conducted, encompassing both academic and industry sources, to extract current C-SCRM methods, challenges, and risk factors. Second, semi-structured expert interviews are held with cybersecurity professionals to validate and refine the proposed best practices. These insights are analyzed using grounded theory to ensure robustness. Finally, the resulting implementation guideline is evaluated against the requirements of the NIS2 Directive to determine its regulatory alignment and practical applicability.

Results: The study produced a consolidated best-practice implementation guideline for Cyber Supply Chain Risk Management. This guideline comprises a structured set of practices organized into four thematic areas (governance, procedures, monitoring, and risk management) and was refined through expert feedback. The expert evaluation of the guideline indicated strong clarity, feasibility, and acceptability, suggesting that it effectively addresses major gaps in existing C-SCRM frameworks. When benchmarked against the EU NIS2 Directive, the guideline was found to cover all key requirements of Article 21.2(d), demonstrating that it not only aligns with regulatory obligations but also provides actionable steps for compliance. Overall, the results confirm that the guideline can substantially lower the practical barriers for organizations (especially those with limited cybersecurity resources) to improve their supply chain cyber risk posture.

Conclusion: The research concludes that C-SCRM challenges can be confronted by bridging disparate best practices into a unified, actionable framework aligned with regulatory mandates. By synthesizing academic insights, industry standards, and expert knowledge, the thesis delivers a practical roadmap that enables organizations to enhance supply chain cybersecurity and meet NIS2 requirements in tandem. This best-practice approach effectively translates high-level recommendations into operational guidance, empowering even smaller enterprises to proactively manage cyber risks in their supply chain. In summary, the developed guideline serves as a relevant and valuable tool that supports regulatory compliance and strengthens overall cyber resilience in an increasingly interconnected supply chain environment.

Acknowledgements

I would like to express my sincere gratitude to my supervisors, J.M.W. Visser and E. Makri, for their structured guidance and valuable feedback, which were essential in elevating this thesis to its final form. I am also deeply thankful to the experts who participated in the interviews, your participation added valuable insights and a new dimension to this work. A special thanks goes to my team at KPMG NL for making my thesis internship such an enjoyable experience. In particular, I would like to thank my manager, Mert Solen, for your time, support, and for providing me with opportunities to further develop myself throughout this process. Finally, I want to thank my friends, family, and girlfriend. Your unwavering support during this journey made it all possible.

Contents

Chapter 1

Introduction

In this chapter, we will provide an overview of the key elements that form the foundation of this thesis. First, the problem statement paints a picture of the current issues and challenges in cyber supply chain risk management that this research aims to address. The research objective details the goal and aim of the study. Next, research questions are provided that structure the research process. The research scope section defines the boundaries and limitations of the study after which the structure of the thesis is outlined.

1.1 Problem statement

The importance of Information Technology (IT) infrastructure has grown over the years. With this, the significance of cybersecurity expanded into Operational Technology (OT) infrastructure [37]. Industry 4.0 is characterized by the integration of digital technologies with industrial and operational processes, an even further convergence of IT and OT [48]. These technologies are frequently supplied by third parties. This results in a cyber supply chain that provides a rise in operational capabilities while the organization becomes more reliant on technology from outside. Thus, organizations are exposed to new cyber threats increasing the need for adequate cybersecurity measures in this new environment [51, 55].

In 2022, the growth rate of the cybersecurity economy was double that of the global economy [35]. "In 2023 it grew four times faster" [31]. However, this fast growth has caused a growing cyber inequity between organizations, specifically smaller organizations are becoming less resilient [31, 32]. This is in part due to an increasing shortage of cyber skills and talents [31, 32]. This inequity, talent shortage, and proliferation of various regulations pose problems for organizations to maintain compliance and security [32]. This underscores the need to establish supportive measures to help organizations navigate compliance challenges and enhance their security posture.

This necessity has also been highlighted by recent attacks focused on the ever-growing supply chain [74, 7]. These attacks utilize a single point of entry in one of the nodes of a supply chain to access the data and systems of multiple organizations connected to it. Having a severe impact on, inter alia: significant financial losses, erosion of consumer trust, and, in some cases, critical disruptions to national infrastructure [3, 7]. In response to this growing risk landscape, legislative bodies try to create a unified security culture across sectors and increase international preparedness [21, 42].

The Network and Information Systems Directive 2 (NIS2) is one of the efforts of the EU to improve this overall cybersecurity posture [20]. NIS2 article 21.2.d explicitly requires entities to manage the risks in their supply chain security. However, some criticism has been raised regarding the practical implementation of these requirements [75, 76, 68]. For example, the broad definition of critical sectors within NIS2 may dilute the focus and effectiveness of cybersecurity measures [76]. Additionally, the directive's broad scope can present unique compliance challenges for organizations facing situations not adequately addressed by the NIS2 legal framework [75]. This underscores the need for organizations to adopt measures independent of legislative requirements to ensure a secure supply chain [76, 68].

Due to the multi-disciplinary nature of Supply Chain Risk Management (SCRM), academia has taken the time to recognize the problems of maintaining a secure supply chain, as they do not clearly belong to

any particular specialty [51]. Industry standards are developed as a form of self-regulation within sectors and to support organizations with regulatory compliance. Renowned institutes such as International Organization for Standardization (ISO) and National Institute of Standards and Technology (NIST) have created highly regarded [61, 75, 9] resources on the subjects of information security management and supplier relationships [45, 12, 13]. However, the creation of various methods and resources across industries and institutions has led to a scattered landscape of best practices, standards, and methodologies. This proliferation of complex and extensive documents poses a significant challenge for most companies to comprehend and implement effectively, particularly smaller organizations that face a shortage of skilled personnel [32].

Taking all this into account, organizations are confronted with an expanding attack surface, a shortage of cybersecurity skills, and a fragmented landscape of methods. Consequently, they face an increasing array of risks, while the available mitigation strategies demand a level of expertise that many organizations lack. This situation makes it challenging for these organizations to develop customized plans with the necessary measures to protect their supply chains. Currently, there is no widely adopted implementation guideline that reduces the entry barrier to protect supply chains through mitigation strategies and assists organizations in establishing an effective Cyber Supply Chain Risk Management (C-SCRM) function.

1.2 Research objective

This thesis creates a guideline for the implementation of best practices in Cyber Supply Chain Risk Management (C-SCRM). This is done by exploring previous academic and industry work and combining them with expert opinions. We evaluate the resulting C-SCRM best practices implementation guideline against the NIS2 requirements on C-SCRM and measure the relationship between both documents. Through this, we determine whether our proposed guideline achieves NIS2 compliance with Article 21.2.d or, conversely, addresses additional areas to mitigate the emergence of supply chain cybersecurity issues.

This research provides a clear overview of best practices for C-SCRM, presented through an implementation guideline. The guideline is designed to lower the expertise required to establish and operate a C-SCRM capability within an organization. This research makes C-SCRM more accessible by offering actionable strategies that enable organizations to enhance their cyber supply chain risk management and address potential vulnerabilities. In doing so, it contributes to the global effort to raise cybersecurity standards across supply chains.

1.3 Research questions

A set of cybersecurity best practices is needed in the C-SCRM domain. This paper has the main goal of proposing such a set of methods in the format of an implementation guideline. This guideline will be the result of the following main research question.

RQ *How to confront the challenges in Cyber Supply Chain Risk Management in accordance with NIS2 article 21.2.d?*

To define an extensive and novel answer to the main research question, the question is divided into a set of sub-questions. Each accounts for a different part of our research problem. Every sub-question answers a step in the process to provide the answer to the main research question with a substantial theoretical base. The identified set of sub-questions is the following:

SQ1 How are C-SCRM methods represented in academic and industry literature?

SQ2 What are the practical limitations of the available C-SCRM methods in literature?

SQ3 How can best practices for C-SCRM be shaped into an implementation guideline?

SQ4 How does our proposed implementation guideline relate to NIS2 article 21.2.d?

The separated method landscape for supply chain risk management needs to be reconciled and harmonized to develop a cohesive and integrated approach that addresses the complexities of cybersecurity in the supply chain. This will be achieved by answering SQ1. This harmonized view will be evaluated

through SQ2 in the form of interviews. In SQ3 we will shape the resulting data into a robust implementation guide for C-SCRM. Through SQ4, we will evaluate our proposed C-SCRM best practices implementation guideline against the requirements of NIS2 article 21.2.d to see how these documents relate to each other in their goal of ensuring cybersecurity in supply chains.

1.4 Research scope

This research is carried out as part of a thesis internship at KPMG NL, more specifically the Strategy & Risk team of the Cyber & Techlaw department. The study is carried out over a 6 month period and focuses on developing a practical implementation guideline for Cyber Supply Chain Risk Management, with particular attention to its alignment with the requirements of the European Union's NIS2 Directive, specifically Article 21.2.d.

The scope of the research is both conceptual and applied. Conceptually, the study encompasses the identification and synthesis of best practices in C-SCRM through an extensive review of academic literature and industry standards. This includes the analysis of widely recognized frameworks and publications from international institutions.

From a practical applied perspective, the research validates and enriches these practices through a series of semi-structured interviews with cybersecurity professionals affiliated with KPMG's global expert network. The emphasis lies particularly on making C-SCRM more accessible to small and mid-sized organizations, which often face challenges in implementation due to limited resources, expertise, or organizational maturity [32].

Certain boundaries are defined to ensure the feasibility of the research. The study is limited to the domain of cyber risk within the context of supply chains and does not consider broader operational, financial, or geopolitical supply chain risks.

The outcome of this research is a structured and actionable implementation guideline intended to serve as an accessible resource for organizations anticipating emerging regulatory requirements and seeking to enhance their supply chain cybersecurity posture. While the study draws on expert knowledge primarily from the KPMG network, the proposed practices are intended to be generalizable across sectors and organizational types.

1.5 Structure

This thesis is structured into seven chapters, each addressing a distinct component of the research process and collectively contributing to the central research question: *How to confront the challenges in Cyber Supply Chain Risk Management in accordance with NIS2 Article 21.2.d?*

- **Chapter 1 - Introduction:** This chapter provides the foundation of the research by outlining the problem statement, research objectives, and research questions. It also delineates the scope of the study and introduces the overall structure of the thesis.
- **Chapter 2 - Method:** The methodological framework adopted in this research is explained in detail. The chapter describes the three-cycle research design: exploration, confirmation, and evaluation, and discusses the specific methods employed, including the literature review, expert interviews, grounded theory analysis, and the comparative mapping to the NIS2 Directive.
- **Chapter 3 - Literature review:** This chapter presents the theoretical grounding for the study. It synthesizes relevant academic literature and industry resources to define key concepts, identify current challenges and risks in C-SCRM, and review existing mitigation approaches. The insights from this review form the basis for the initial formulation of best practices.
- **Chapter 4 - Best practice implementation guideline:** This chapter introduces the final implementation guideline, structured around a series of actionable best practices. Each practice is described in terms of its objective, applicability, implementation considerations, and contribution to improving supply chain cybersecurity.
- **Chapter 5 - Interview results:** The findings from semi-structured expert interviews are presented and analyzed. This chapter explores practitioners' perspectives on the practical challenges

and limitations of existing C-SCRM methods and presents expert feedback on the draft guideline captured via the FACE framework.

- **Chapter 6 - Discussion:** The research findings are critically evaluated in this chapter. It compares academic and industry insights, reflects on the strengths and limitations of the proposed guideline, and assesses the degree to which it aligns with the requirements of NIS2 Article 21.2.d.
- **Chapter 7 - Conclusions:** The concluding chapter summarizes the main findings, answers the research questions, and highlights the academic and practical contributions of the study. It also outlines recommendations for future research to focus on further evaluating the implementation guideline in diverse organizational settings, assessing its real-world impact, and exploring ways to enhance its accessibility, stakeholder alignment, and regulatory integration.

Chapter 2

Methodology

This research consists of three cycles that involve separate research methods as indicated in Figure 2.1. During the first cycle, Exploration, a literature review is conducted to establish a theoretical foundation in the domain of C-SCRM. Through this analysis we gather data that is used to answer sub-question 1 (SQ1). Based on the literature, we draft our initial set of best practices. The second cycle, Confirmation, will primarily consist of expert interviews. On the one hand, the interviews are used to gain additional insight into the challenges and barriers in the security of supply chains, making this cycle partly exploratory. On the other hand, the interviews validate our findings from cycle one, making it confirmatory in nature. This approach is used to identify any limitations of the C-SCRM methods identified in the Exploration cycle to answer SQ3. With the data from these two cycles we form our final best practices implementation guideline. The last cycle, Evaluation, consists of an evaluation phase where the proposed guideline is evaluated against the requirements of NIS2. This chapter discusses the different methods utilized in these three cycles.

	Cycle 1: Exploration	Cycle 2: Confirmation	Cycle 3: Evaluation
Description	Establishes the theoretical foundation by reviewing academic and industry literature.	Validates and enriches initial findings through expert interviews	Assesses the guideline's alignment with NIS2 regulatory requirements
Research products	• Categorized findings on C-SCRM from academic literature • Overview of provided guidance from industry resources • Initial best practices implementation guideline	• Contextual challenges and implementation barriers • Final best practices implementation guideline	• NIS2 mapping document
Research methods	• Literature review	• Semi-structured interviews • Grounded theory analysis	• Comparative mapping • Gap analysis
Research question answered	• **SQ1:** How are C-SCRM methods represented in academic and industry literature?	• **SQ2:** What are the practical limitations of the available C-SCRM methods in literature? • **SQ3:** How can best practices for C-SCRM be shaped into an implementation guideline?	• **SQ4:** How does our proposed implementation guideline relate to NIS2 Article 21.2.d?

Main RQ: How to confront the challenges in Cyber Supply Chain Risk Management in accordance with NIS2 Article 21.2.d?

Figure 2.1: Overview of our research cycles, outlining the delivered research products, used methods, and answered research questions per cycle.

2.1 Literature review

This section outlines the process followed for our literature review.

2.1.1 Academic literature selection

Academic articles used in the literature review were sourced using a combination of Google Scholar search engine, Consensus search engine [22], and Research Rabbit [65].

For the purpose of this research, the criteria for including an academic article in the literature review are the following:

- The main theme of the work is either SCRM, Third-party risk management or C-SCRM.
- The work identifies a set of C-SCRM challenges, risks, sources of risk, measures, or concepts.
- The work is published in English.

The Google Scholar search engine is used to find an initial set of articles. Google Scholar was selected for its broad coverage of scholarly literature across disciplines, making it a reliable starting point for identifying foundational works. Keywords and key phrases were used to filter through the vast number of records available through the search engine. The search queries incorporated keywords and key phrases such as Supply Chain Risk Management, Supply Chain, Cybersecurity, SCRM, C-SCRM, TPRM, Third-Party, Third-Party Risk Management and Cyber Supply Chain Risk Management. This list of keywords and key phrases is used to incorporate relevant articles utilizing different variations of terminologies.

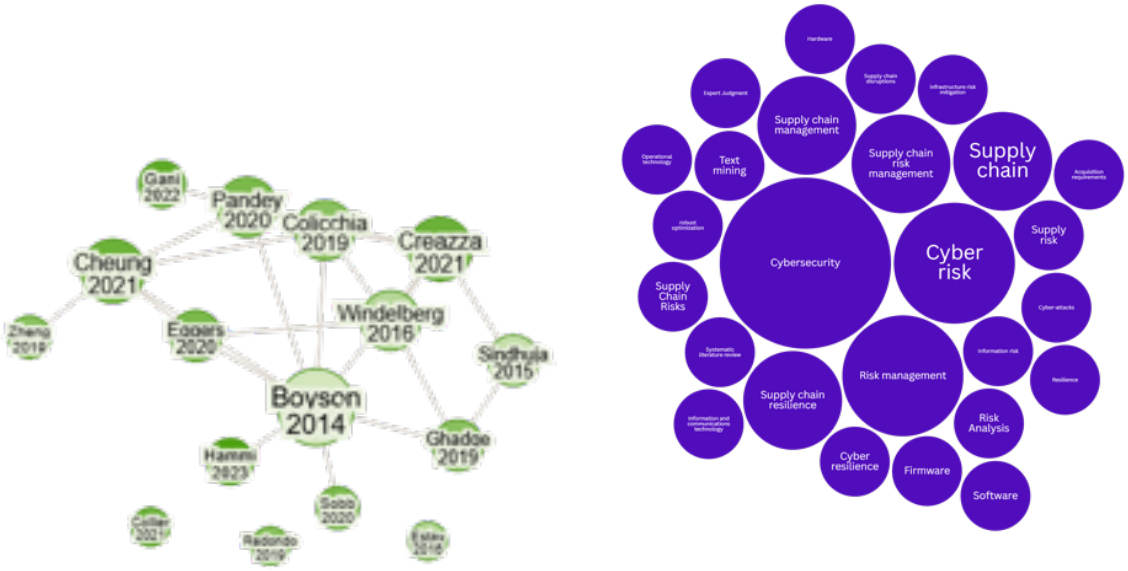
Additionally, works are elicited through the Consensus search engine [22]. Consensus was used to supplement the set found through Google Scholar by leveraging its natural language processing to identify highly relevant peer-reviewed articles within the C-SCRM domain, some of which were not easily discoverable through keyword-based searches alone. This is done using the following prompts:

- *"Please give sources for a literature review of works discussing methods for cyber supply chain risk management."*
- *"What are successful methods for cyber supply chain risk management?"*

Because of incidental hallucinations and the inconsistent nature of AI tools we execute these prompts three times within the Consensus search engine to ensure minimal deviation between answers is given.

The articles aggregated from these two sources are then added to the Research Rabbit platform [65]. Research Rabbit is used to keep track of all aggregated articles. Additionally, it is used to identify connected papers through visual mapping of citations, employing both forward and backward snowballing techniques. This provides an intuitive process for discovering new relevant articles and visualizing connections between the works included in our literature review.

Using a combination of these tools makes the selection of a complete set of articles fit for comprehensive literature review more intuitive, and efficient.



(a) Network representation of articles included in our literature review, generated by Research Rabbit [65].

(b) Keyword visualization of cyber supply chain risk management literature, generated with Flourish [30].

Figure 2.2: Data visualization of the set of 20 articles comprising our literature review

From these sources, 20 resulting articles are used in our literature review. These articles, dating back to 2014, are displayed in Table 2.1. Figure 2.2a was generated using Research Rabbit [65] and shows our selection of articles and their relationships with each other. The lines in the figure represent citation links, where one paper references another. Bigger nodes indicate publications that reference more papers or are cited by more papers within our selection. The citation-network displayed by Figure 2.2a shows strong interconnection within our selection, with the exception of three outlier articles, Collier and Sarkis [19], Redondo et al. [66], and Estay and Khan [26], which do not have any citation links to the other papers in our dataset.

Figure 2.2b shows the visualization of the author-supplied keywords indicated in our selection of articles. The figure is generated by aggregating all keywords indicated per article, standardizing variations of the same keyword (e.g., 'cyber-risk' and 'cyber risk'), counting the occurrences of each keyword, and then visualizing the data as a packed circles hierarchy map using the online tool Flourish [30]. The size of a dot in the figure increases with the occurrence of the associated keyword. In total, our selection of 20 articles features 39 keywords, of which 26 remain after standardizing, which are displayed in Figure 2.2b. This overview shows that most articles take a risk-focused approach with 7 unique keywords featuring the word risk.

These metrics show the interconnected nature of the selected literature and the dominant themes within our review. The strong citation relationships among most papers indicate a cohesive body of research, highlighting the relevance of our selection. Additionally, the keyword analysis shows a dominant emphasis on risk-related topics, suggesting that risk assessment and mitigation are central concerns in the analyzed articles.

Article	Year	Author	Title
1	2019	Colicchia et al. [18]	Managing cyber and information risks in supply chains: insights from an exploratory analysis
2	2019	Ghadge et al. [36]	Managing cyber risk in supply chains: A review and research agenda
3	2019	Zheng and Albert [82]	A robust approach for mitigating risks in cyber supply chains
4	2023	Alanazi and Solangi [5]	Cyber Supply Chain Risk Management: A Conceptual Model
5	2019	Redondo et al. [66]	Assessing Supply Chain Cyber Risks
6	2016	Windelberg [79]	Objectives for managing cyber supply chain risk
7	2016	Estay and Khan [26]	Control structures in supply chains as a way to manage unpredictable cyber-risks
8	2014	Boyson [15]	Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems
9	2022	Creazza et al. [23]	Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era
10	2022	Gani et al. [34]	Interplay between cyber supply chain risk management practices and cyber security performance
11	2024	Jazairy et al. [47]	Cyber risk management strategies and integration: toward supply chain cyber resilience and robustness
12	2021	Collier and Sarkis [19]	The zero trust supply chain: Managing supply chain risk in the absence of trust
13	2020	Pandey et al. [58]	Cyber security risks in globalized supply chains: conceptual framework
14	2021	Eggers [25]	A novel approach for analyzing the nuclear supply chain cyber-attack surface
15	2024	Abrahams et al. [1]	Reviewing third-party risk management: best practices in accounting and cybersecurity for superannuation organizations
16	2023	Hammi et al. [41]	Security threats, countermeasures, and challenges of digital supply chains
17	2015	Sindhuja and Kunnathur [69]	Information security in supply chains: A management control perspective
18	2024	Adenekan et al. [3]	Strategies for protecting IT supply chains against cybersecurity threats
19	2021	Cheung et al. [17]	Cybersecurity in logistics and supply chain management: An overview and future research directions
20	2020	Sobb et al. [70]	Supply chain 4.0: A survey of cyber security challenges, solutions and future directions

Table 2.1: The selection of academic articles adopted in our literature review, ordered by discovery and inclusion during the research process.

2.1.2 Academic literature analysis

From the corpus of literature collected, we extracted insights within the categories of identified C-SCRM challenges, risks, sources of risks, and measures. We chose these categories because they encompass the critical dimensions necessary for a comprehensive understanding of C-SCRM. By examining challenges, we identify the obstacles that organizations face in implementing effective C-SCRM strategies. This analysis helps to pinpoint specific areas where improvements are needed and provides a foundation for developing targeted strategies. Investigating risks allows for a deeper understanding of potential threats and vulnerabilities within the supply chain. This category is crucial because it highlights the various ways in which supply chains can be compromised. Analyzing sources of risks helps to understand the origins

of these threats. By identifying the driving forces, it is possible to develop more effective prevention and mitigation strategies. By collecting insights in these categories, we can shape our guideline to address the multifaceted nature of C-SCRM. This comprehensive approach ensures that our guideline is well-rounded and grounded in academic research.

Insights are gathered by first collecting data on each of the categories per research article. Appendix C shows the raw data gathered from each paper, outlining the challenges, risks, sources of risks, and measures mentioned in each of the analyzed articles. This data is then consolidated into themes and sub-themes per category by eliminating synonymous terms and concepts and creating broader themes where needed. Due to varying levels of detail used in the literature per identified theme, some themes feature sub-themes, while some do not. By maintaining a theme and sub-theme structure we aim to provide a more structured analysis and reporting methodology. Section 3.2 discusses each of the four categories, their (sub-)themes and the specific insights gathered from each of the articles within these (sub-)themes. This overview gives us a broader understanding of academic perspectives on the current state of C-SCRM. Through this we can substantiate the recommendations in our best practices implementation guideline with academic data. Section 2.3 further discusses how the insights gathered from this analysis are processed into our best practices implementation guideline.

2.1.3 Industry resource analysis

Organizations such as NIST and ISO have produced several industry resources and standards that cover a wide variety of aspects of C-SCRM. Industry standards are tools that can enable the achievement of numerous benefits across various sectors by facilitating knowledge exchange, improving process integration, and enhancing collaboration [81, 6, 73, 29].

We identified a set of industry resources that include procedures, implementation guidance, standards, and recommendations in the domain of C-SCRM. The works of Boyens et al. [12] and Bartol [9] already analyzed available C-SCRM resources and outline a set of reputable sources. From these we selected resources that offer general C-SCRM requirements or foundational security practices. By studying these works, we can supplement the insights gathered from the academic literature to further substantiate our best-practices implementation guideline.

The industry resources adopted in this research emanate from three different institutes:

- International Organization for Standardization (ISO)
- National Institute of Standards and Technology (NIST)
- European Supervisory Authorities (ESAs)

Section 3.3 offers an in-depth overview of each industry resource utilized, highlighting the background and unique insights provided by each source. It concludes with a comprehensive mapping of these resources to the specific best practices that form our implementation guideline, detailing the origins of the insights that support our guideline. Section 2.3 gives a more detailed explanation on how these resources are reshaped into our final guideline.

Table 2.2 shows the list of industry resources included in our literature review along with the following information for each resource [12]:

- Scope: specific sector of the acquirer or a type of supplier that is being sought
- Audience: whether the resource speaks to both acquirers and suppliers
- Context of use: high-level summary of what the resource provides

Document	Scope	Audience	Context of Use
NISTIR 8276, Key Practices in Cyber Supply Chain Risk Management: Observations from Industry	Any	Acquirers and Suppliers	Key practices and recommendations for managing cyber supply chain risks across various industries
NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations	Federal [USA] information systems	Acquirers	Identifying, assessing, and mitigating ICT supply chain risks
ISO/IEC 27002: Code of practice for information security controls	Any	Acquirers and Suppliers	Guidance for implementing security controls in support of information security management system in ISO/IEC 27001
2015/2019 Case Studies – NIST Best Practices in Cyber Supply Chain Risk Management:	Any	Acquirers	Industry best practices
DORA RTS 84, Regulatory Technical Standards on ICT risk management framework	Financial sector	Acquirers	Harmonising ICT risk management tools, methods, processes, and policies across the financial sector
DORA RTS 86, Regulatory Technical Standards on the policy on ICT services supporting critical or important functions provided by ICT third-party service providers	Financial sector	Acquirers	Governance, risk management, and internal control framework for ICT third-party service providers

Table 2.2: Overview of the various C-SCRM industry resources included in our literature review. This overview is largely sourced from Boyens et al. [12] and expanded with data on the DORA RTS documents.

2.2 Best practices format

The goal of this research is to develop a best practices implementation guideline. A universally accepted method for identifying best practices does not exist, and authors vary in the scope and characteristics used [60, 16, 80, 38]. Our proposed best practices are established through a combination of literature review and expert interviews. Herein we follow the approach of Peters and Heron [60] where best practices are intended to be a useful means of organizing literature to highlight key empirical findings and to outline practices that are proven effective, valued by the field, or likely to achieve desired outcomes. Peters and Heron [60] outline criteria for defining best practices in line with this. They emphasize that best practices ought to be rooted in a robust theoretical foundation through a "Sound Theoretical Base" and "Consensus with Existing Literature". We achieve this through our comprehensive literature review. Additionally, the "Social Validity" criterion stresses the necessity of seeking validation through a representative sample belonging to the group intended for these best practices. In our research, this is partially attained through expert interviews that validate our initial findings and provide further insights. Chapter 5 will discuss potential improvements in this area.

Moreover, Peters and Heron state that best practices should define their "Desired Outcomes Produced", making it clear what the goal is of implementing a certain best practice. This means that throughout our implementation guideline, an explanation is provided for why certain practices should be implemented and what results could be expected. This is accompanied by a clear description of how to implement each measure and in what order, providing a well-structured and compelling methodology to apply the best practices. In the context of this research, this satisfies the criterion of having a "Convincing and Compelling Methodology and Design" to support the best practices. This approach ensures that our research results are more than just a checklist [60]. By adhering to the criteria proposed by Peters and Heron, we ensure that our research results are theoretically sound, clearly defined, and validated by industry experts, making them robust and reliable.

Furthermore, the selection of practices as "best" practices should be done through defined criteria [60, 80, 16]. Wu et al. [80] propose a set of values that are valued as being effective in guiding the process of selecting best practices:

- **Replicability:** Refers to the need for best practices to be generalizable, applicable to other locations and conditions, and accompanied with helpful guidelines for others to follow.
- **Effectiveness:** Practices that are expected to have more effect [compared to other practices] in minimizing risks in supply chains are a key characteristic in selection.
- **Sustainability:** The implementation guideline is shaped to make operation possible over a period of time. Taking into account the financial, social, and political factors determining cybersecurity policies.
- **Innovativeness:** The implementation guideline aims to include a novel set of relevant and adaptable best practices, avoiding redundancy and promoting creative solutions to emerging challenges.

These values guide our approach of shaping the implementation guideline and selecting practices as "best" practices. The method used to document best practices should incorporate these values and the previously mentioned criteria. Whited et al. [78] propose such a documentation method that follows a structured approach. This method was defined in the context of transportation project management, but is generalized and applicable to various domains. This structured approach, along with its constituent elements, supports the adoption of the aforementioned criteria and values, thereby aligning with the objectives of this research. The following elements are used to organize and document each best practice:

Aspect	**Description**
Title	The name of the best practice.
Brief Description	A concise summary of the best practice.
Additional Details	Information to aid in the implementation of the best practice.
Objective	The primary goal or purpose of the best practice.
When to Apply	Situations or conditions under which the best practice should be used.
Cost Implications	The financial considerations associated with implementing the best practice.
Conditions for Successful Application	The necessary conditions or prerequisites for the best practice to be effective.
Cautions	Potential risks or issues to be aware of when applying the best practice

Table 2.3: Elements for best practice definition [78].

Through this approach, best practices form a medium for increasing awareness by effectively translating research into a form that meets the needs of management and decision-makers [60]. By defining best practices, attention can be focused on fundamental information that should influence behavior [60]. Identified best practices can highlight the need for system change, financial support, dissemination, and training [60].

2.3 Best practice implementation guideline development

Converting standalone best practices into an inter-linking and effective implementation guideline involves several key requirements. One critical requirement is implementability, which is essential for real-world adoption [49, 33]. Research in the domain of clinical practices shows that this involves three key enablers of implementability: stakeholder involvement, evidence traceability, and feasibility of implementation [49].

In line with this, the proposed guideline explicitly assigns responsibility for implementing specific best practices or entire sections, thereby embedding accountability into the framework. The recommendations are grounded in evidence collected from both the literature review and expert interviews, and each recommendation is clearly mapped back to its evidence base to ensure traceability.

To ensure feasibility, we adopt implementation-focused design principles recommended by Kastner et al. [49], including:

- Formulate recommendations in terms of measurable criteria and targets for quality improvement
- Identify costs and resource requirements
- Specify competencies, training, and technical specifications required

Gagliardi and Brouwers [33] states that the developers of guidelines should ensure that they are practical and applicable in real-world settings. Guidelines should include detailed implementation advice to enhance the guidelines' practical application [33]. While our independent best practices are designed to guide the audience in implementation and decision making, the guideline organizes these practices into a cohesive process. Each new practice builds upon the previous one, creating an interconnected sequence from start to finish.

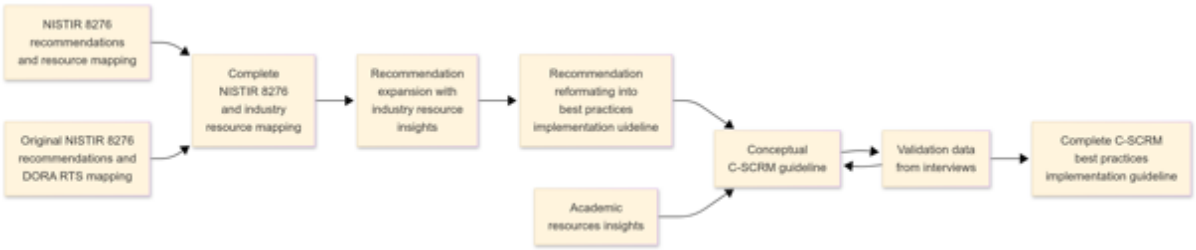


Figure 2.3: Development pipeline of our best practices implementation guideline.

Figure 2.3 provides an overview of the entire development pipeline used in this research to create our guideline. Our best practice implementation guideline builds on the insights discovered in our literature review. We start by identifying best practices from industry resources. The NISTIR 8276 [12] is an influential document in the structuring of this process. The document presents a set of eight C-SCRM key practices in the form of high-level concepts, combined with a list of 24 recommendations on how organizations can put the key practices to use. Since NISTIR 8276 [12] only offers high-level guidance for implementing a C-SCRM function and refers to other resources for guidance on how to further implement these recommendations, it requires a certain level of knowledge, skills, and resources to create a holistic approach fit for a specific organization. Implementing advanced tools and technologies at this level requires expertise that is lacking in a lot of organizations [18, 32].

We create a more holistic approach to C-SCRM by taking the list of 24 recommendations from NISTIR 8276 [12] and directly expanding them with the implementation guidance found in the other industry resources as outlined in Section 2.1.3. NIST IR 8276 [12] provides a mapping between its 24 recommendations and several industry resources that provide more information on how to implement them. This mapping features the first three industry resources adopted in our analysis. We expand this mapping with our own original mapping between the recommendations and specific articles from DORA RTS 84 & 86. From here we start aggregating insights on how to implement these recommendations based on the industry resources. The complete mapping between the recommendations and industry resources, along with the specific insights gathered from each industry resource, can be found in Section 3.3.

To convert these data into interlinking best practices that form a complete implementation guideline, we needed to reformat the recommendations, group them into categories, and order them to provide guidance on the sequentiality of their implementation. This creates a step-by-step guide on how to establish a C-SCRM function, in the form of a best practice implementation guideline. To provide traceability on the transformation process from the 24 recommendation provided by NISTIR 8276 and our final guideline, Section 6.4 offers a direct mapping between the recommendations and our best practices along with additional explanation of this process.

This structure is then complemented by the insights gathered from the academic literature as discussed in Section 3.2. Although, the findings in the categories of challenges, supply chain risks, and sources of risks are fundamental in understanding the scope of C-SCRM only the data from the category of measures are directly used in the creation of our best practice implementation guideline since it offers the methods that can support establishment of a C-SCRM function. Section 6.4 maps measures found

in our review of the academic literature to the best practices and discusses choices made in this process. Through this process we combine all resources to arrive at a more accessible format that lowers the level of expertise needed to tailor its recommendations to an organizations needs. The resulting best practice implementation guideline is then refined by gathering feedback on the perceived practical implications of the guideline through the execution of expert interviews.

2.4 Interviews

The findings from our literature research must be validated and supplemented with additional insights into the challenges and differences in the security of supply chains. To achieve this, understanding different perspectives, experiences, and beliefs is relevant [24]. This expertise is best acquired through engagement with industry experts. Given the scarcity of specialists in this area and the need to extract maximum insight from these experts, we opt to use interviews as the primary method. Interviews are widely used in exploratory research designs that utilize qualitative methods [24].

2.4.1 Structure

These interviews are used to solicit new approaches for C-SCRM that are not yet covered in the literature. Simultaneously, expert views are gathered on the data from the literature research as a form of additional exploration and verification. The interviews are conducted using a semi-structured approach, ensuring that the questions are supported by the relevant literature. Semi-structured interviews adhere to set guidelines while allowing flexibility to refine questions or explore new themes as the interview progresses [2]. This flexibility is valuable when existing questions no longer yield novel insights or when diving deeper into certain topics.

The interviews are made up of a series of mostly open-ended questions to capture qualitative data. This type of question facilitates innovative and divergent thinking, which is highly beneficial for both the validation and the exploration processes [46]. Some inspiration for structuring these questions has been taken from previous research by Verschuur [77]. The interview questions from this research, which focused on assessment of IoT-based environments, where adapted to fit the purpose of this research while building on existing methods from similar research. the complete interview guide used in the interviews can be found in Appendix B. To identify the overarching patterns within the responses, we use analysis based on grounded theory [71].

To collect expert insights on the domains of C-SCRM challenges, risks, sources of risks, and measures, as explored in our review of the academic literature, interview questions were designed to probe participants on these specific areas. This is done to explore if the expert perspectives align with the patterns observed in academic literature.

Next, we explore the interviewee's familiarity with existing guidelines and frameworks related to C-SCRM, their practical experience in applying these methods, and any specific challenges or gaps they have encountered. These questions help us understand their personal experience with using existing guidance materials and, through that lens, identify potential limitations within those materials.

This is followed by a demonstration of the developed implementation guideline. The demonstration starts with a walkthrough of the 17 actionable titles of the best practices and the visual overview as presented by Figure 4.1. During this step we refrain from going into detail and discussing the specific content of each best practice apart from the titles. This initial high-level overview is designed to prevent information overload and to prompt discussion on the overall structure and approach of the guideline.

Depending on the interviewees domain of expertise and their responses, a subset of best practices is then explored in greater detail. Due to time constraints and the need to maintain participant engagement, only a portion of the guideline is reviewed per interview. However, coverage of the entire guideline is ensured across the full set of interviews by tracking which best practices are discussed in each session.

To complement the qualitative data with quantitative insights, the FACE instrument [63] is used to evaluate expert perceptions of the guideline. This is a structured evaluation framework that examines stakeholder responses along five implementation dimensions: Feasibility, Acceptability, Cost, Equity, and Intent-to-Implement.

Feasibility assesses whether the proposed guideline can realistically be implemented within existing organizational structures and resources. Acceptability examines how well the guideline aligns with the values, needs, and expectations of stakeholder. Cost considers both perceived financial implications and the resource burden associated with implementation. Equity evaluates whether the guideline is perceived to positively improve inclusivity and possible inequality between different stakeholder groups. In the original healthcare context of the FACE instrument, this meant to reflect on whether interventions impact marginalized groups that face structural barriers to health and healthcare and possible exclusion from the health system. In our use case, this variable serves another function, to measure whether our interviewees perceive the developed guideline to positively impact the growing inequality in cyber-resilience between larger and smaller companies, as discussed in Section 1.1. Lastly, Intent-to-Implement measures the likelihood that stakeholders would actually adopt and apply the guideline in practice.

Interviewees are asked to rate the guideline across these dimensions using a standardized set of Likert-scale questions. This allows for systematic comparison of perceived strengths and implementation barriers. This approach provides a validated and replicable mechanism for gauging stakeholder alignment and identifying potential contextual challenges to real-world adoption. The original FACE instrument was developed by the GRADE Working Group, to systematically capture insights from diverse stakeholders (clinicians, patients, public health workers) to guide the implementation planning of clinical practice guidelines. This means that the standardized set of Likert-scale questions is formulated in the context of healthcare. For the purpose of this research we modified these questions to better fit the domain of C-SCRM. These reformulated questions can be found in Appendix B.

2.4.2 Sample

All interviewees for this research are selected from the global KPMG expert network. Although these experts have extensive knowledge of C-SCRM across industries and sectors, their shared connection to KPMG has an impact on the diversity of included environments in terms of type, size, revenue, and viewpoint. In total, 8 interviews were conducted with professionals holding roles across governance, risk, compliance, and technical domains. Additionally, there is a variation in years of experience which results in a differing amount of C-SCRM related projects in which each participant has worked. Table 2.4 presents an overview of the different roles, years of professional experience, subject of education and countries each interviewee has worked in.

Expert	Role	Experience	Education	Country
1	Manager cyber strategy and risk	7,5 years	Management information security systems	TR/NL
2	Policy officer for Dutch municipality	7,5 years	Business administration	NL
3	Information security specialist for financial services company	1,5 years	Information technology	CN/NL
4	Senior associate cyber security	3 years	Cybersecurity	US
5	Senior manager cyber privacy strategy and governance	9 years	Computer science	CN/BE
6	Partner cyber strategy and risk	25 years	Computer Science	NL
7	OT security and incident response expert	Confidential	Confidential	Confidential
8	Technical director EMEA for IT-services organization	30 years	Law	DE

Table 2.4: Overview of interview participants. Expert 7 requested to have personal information excluded from this research.

All interviews were conducted virtually and in English. This has been done due to limited traveling capabilities and to ease the transcription and coding processes. The average duration of the interview

was: 80 minutes, ranging between 48 and 121 minutes.

2.4.3 Grounded theory

For the coding process, we use grounded theory [72]. This methodology allows us to interpret the data from our interviews as objectively as possible. The theory provides clear guidance on how to analyze and validate interview findings. The grounded theory process consists of the following steps [40]:

1. Identify the substantive area.
2. Collect data pertaining to the substantive area.
3. Open code the data during collection.
4. Write memos throughout the entire process.
5. Conduct selective coding and theoretical sampling.
6. Sort memos to find the theoretical code(s) which best organize the substantive codes.
7. Read the literature and integrate with theory through selective coding.
8. Write up the theory.

Open coding is the practice of identifying the most important concepts discussed in the data. This creates a list of codes that highlights all relevant topics to discuss in later stages of the research. These codes can be used to build a robust theory by organizing the findings into a structure of concepts, subcategories, and categories.

In grounded theory, intermediate labeling is the process of labeling the data from each interview before the next is executed [10]. The technique extracts valuable insights and concepts after each interview. This allows for possible modification of the interview questions, allowing for further exploration of topics that elicited significant interest in prior conversations. Using this technique, we avoid the common stage in research progression in which the emergence of new properties or connections ceases during analysis [71]. In contrast, we are able to adapt the structure of subsequent interviews to continue uncovering new pertinent observations. Theoretical saturation of categories is achieved when existing labels or properties are continuously observed and the emergence of new ones ceases [72].

2.5 Implementation guideline and NIS2 analysis

In order to see if our developed guideline holds regulatory validity we benchmark it to the Network and Information Systems Directive 2 (NIS2). NIS2 is the harmonizing legislative instrument for cybersecurity within the European Union, setting minimum requirements for risk management practices and reporting obligations across critical and highly critical sectors [20]. Specifically, Article 21(2)(d) mandates that essential and important entities address supply chain and supplier relationship risks, thereby establishing a legal expectation for organizations to embed C-SCRM practices into their cybersecurity strategies.

By aligning the guideline with the obligations outlined in NIS2, this thesis ensures that its recommendations are not only practically relevant but also legally grounded within the current EU regulatory landscape. We chose NIS2 over other legislation for this benchmarking because of its broad scope and strong relation with supply chain management [76]. Where legislation such as DORA only covers the financial sector, NIS2 impacts a broader range of organization in differing sectors. Furthermore, DORA offers explicit implementation guidance through it's collection of RTS documents while there currently does not exist specific guidance on how to implement a C-SCRM function aligned with NIS2.

The benchmarking is done by comparing our guideline with the C-SCRM requirements under NIS2. While Article 21(2)(d) of the NIS2 Directive is the only clause that explicitly mandates the management of cybersecurity risks in supply chains and supplier relationships, it does not operate in isolation. In reality, effective C-SCRM is implicit in several other provisions of NIS2, even if not directly named. This means that to fully evaluate the alignment of our implementation guideline with NIS2, it is necessary to adopt a broader interpretation of the directive's requirements for C-SCRM.

Table 2.5 outlines all explicit and implicit C-SCRM obligations we identified throughout the NIS2 directive mapped to the specific articles and recitals relevant to each requirement. We can compare our

guideline to this overview to benchmark it's legal position. The results of this benchmarking are presented in Section 6.3.

The table was created through a close reading and annotation of the NIS2 Directive, particularly Articles 20 to 23 and relevant recitals (e.g., 82–90). Each requirement was extracted by identifying recurring themes such as vendor risk assessment, contractual control, incident handling, and fourth-party risk.

Where needed, multiple articles and recitals were cross-referenced to fully capture the intent behind a given requirement. To strengthen validity, these interpretations were reviewed against regulatory commentary and expert analysis referenced earlier in this thesis (e.g., [75, 76, 68]). As a result, the table offers a comprehensive and traceable mapping of all explicit and implicit C-SCRM obligations in NIS2.

Requirement	Explanation	NIS2 Directive Reference
Comprehensive risk assessment	Assess all vendors' risks, classify by criticality, and update regularly.	**Art. 21(1) & 21(2)(a):** Requires risk analysis and security policies. **Art. 21(2)(f):** Requires procedures to assess effectiveness of risk measures (continuous re-assessment). **Rec. 85:** Emphasizes assessing suppliers' overall cybersecurity quality and resilience.
Supply chain security policies	Implement security controls for supplier relationships, ensure suppliers meet cybersecurity standards.	**Art. 21(2)(d):** Mandates supply chain security measures for relationships with direct suppliers/providers. **Art. 21(3):** Must consider each supplier's vulnerabilities and practices when adopting measures. **Rec. 85:** Highlights importance of addressing supply chain risks in policies.
Incident reporting & response	Establish incident handling for third-party incidents and report significant incidents timely.	**Art. 21(2)(b):** Requires incident handling processes (covers third-party incidents affecting the entity). **Art. 23(4):** Reporting timeline - 24h initial notification, 72h report, etc., for significant incidents. **Rec. 85:** Notes many incidents originate via third parties (rationale for strict reporting).
Continuous monitoring & evaluation	Ongoing vendor security monitoring, periodic audits, and threat updates.	**Art. 21(2)(f):** Continuous evaluation of cybersecurity measures (implies ongoing vendor audits/monitoring). **Art. 21(3):** Incorporate new info (e.g. results of EU supply-chain risk assessments) into risk management. **Rec. 88:** Entities should address risks in interactions within their ecosystem and apply measures when using third-party data/services. **Rec. 89:** Calls for entities to evaluate and improve their cybersecurity capabilities over time.
Documentation & auditability	Keep records of C-SCRM activities and be ready for compliance audits.	**Art. 21(2):** Implies documented policies/procedures for risk management and supplier security. **Art. 32(2)(e) & (g):** Authorities can request documented policies and evidence of cybersecurity measures. **Art. 20(1):** Management must approve and can be held liable for cybersecurity measures.
Contractual obligations on suppliers	Include cybersecurity clauses (compliance, reporting, audit rights, termination) in vendor contracts.	**Rec. 85:** Encourages integrating cybersecurity risk-management measures into contracts with suppliers. **Art. 21(2)(d):** Supply chain security measure provides legal basis to enforce security requirements on suppliers. **Art. 21(3):** Considering supplier practices may necessitate contractual access to info about those practices.
Management responsibility	Executive oversight and accountability for third-party cybersecurity.	**Art. 20(1):** Management bodies must approve and oversee risk-management measures (including C-SCRM) and are liable for non-compliance. **Art. 20(2):** Management required to undergo cybersecurity training. **Rec. 82:** Stresses proportional measures based on risk exposure and impact.
Training & collaboration	Train staff (and encourage suppliers) on cybersecurity; collaborate on threat info and best practices.	**Art. 21(2)(g):** Requires cyber hygiene and training programs. **Art. 20(2):** Mandates training for management and encourages it for all employees. **Art. 29:** Enables cybersecurity information-sharing arrangements. **Rec. 89:** Urges regular staff training and awareness. **Rec. 88:** Advises securing cooperation with external stakeholders.
Fourth-party risk	Manage risks posed by subcontractors and upstream supply chain.	**Rec. 85:** Entities should consider risks from "other levels of suppliers and service providers." **Art. 21(2)(d):** Indirectly points to assessing the chain of critical dependency. **Art. 22 & Rec. 90:** Coordinated risk assessments identify deep-tier supply chain risks.

Table 2.5: Overview of NIS2 requirements in the domain of C-SCRM.

Chapter 3

Literature review

This section displays the necessary theoretical base upon which our best practice implementation guide is built. By examining previous work originating from both academia and industry, we can formulate a state-of-the-art set of best practices needed for C-SCRM.

3.1 C-SCRM definitions

Before dissecting the corpus of literature adopted in this research, we determine certain common definitions to increase clarity and consistency. These definitions guide us in better understanding the field of C-SCRM and the challenges associated with it.

The National Institute of Standards and Technology (NIST) defines the *supply chain* as a "linked set of resources and processes between multiple tiers of developers [entities involved in creating or delivering products and services] that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer" [67]. This definition highlights the complex, multi-tiered structure of modern supply chains, which introduces numerous inter-dependencies and potential points of failure. Similar approaches to this definition are adopted in academic work published on the subject [17, 36, 3, 1].

Management of the risks arising from this complexity is the relatively new and fast-growing domain of Supply Chain Risk Management (SCRM) [64]. One common definition of *SCRM* describes it as: "the management of risk that implies both strategic and operational horizons for long-term and short-term assessment. It refers to risks that can modify or prevent part of the movement and/or efficient flow of information, materials and products between the actors of a supply chain within an organization, or among actors in a global supply chain (from the supplier's supplier to the customer's customer)" [11, 50]. This definition is particularly relevant for understanding the breadth of SCRM. It involves both upstream and downstream risks and stresses the need for visibility across organizational boundaries. Importantly, it integrates both operational and strategic concerns, acknowledging that disruptions may stem from day-to-day inefficiencies or from more structural, long-term vulnerabilities.

Within this broader discipline, Cyber Supply Chain Risk Management (C-SCRM) lies on the intersection of cybersecurity and SCRM, where cybersecurity risks within the supply chain context are confronted [8]. ICT/OT users depend on a complex, global supply chain ecosystem involving multiple entities and tiers of outsourcing [56]. This ecosystem includes IT, OT, Communications, IoT, and Industrial IoT, and it manages the entire lifecycle of products and services [56]. C-SCRM focuses on identifying, assessing, and mitigating risks in these interconnected supply chains [56]. It covers all stages from design of a product or service to termination of a supplier relation [56]. The overall goal of *C-SCRM* is best describes as: "ensuring the integrity, security, quality, and resilience of the supply chain and its products and services" [56].

To fully understand this domain, it is essential to distinguish between three foundational concepts within C-SCRM: threats, vulnerabilities, and risks. A threat refers to any circumstance or event with the potential to adversely affect supply chain operations, systems, or data. *Threats* can be "adversarial" like supply chain attacks or counterfeits, or "non-adversarial" like natural disasters or poor quality [56]. A

vulnerability is a weakness or flaw in systems, processes, people, or relationships that may be exploited by a threat. These can be "internal", such as organizational procedures, or "external", such as an organization's supply chain partner [56]. A *risk* in this context is the measure of the adverse impacts of these threats or vulnerabilities potentially manifesting [56].

A common example of a threat that exploits a vulnerability are *supply chain attacks*. Lust [54] define a these type of attacks as: a "compromise of a particular asset, e.g. a software provider's infrastructure and commercial software, with the aim to indirectly damage a certain target or targets, e.g. the software provider's clients. This type of attack is typically used as a first step in a series of attacks. More concisely, it is used as a stepping stone for further exploitation, once foothold is gained to the target system or systems". Ludvigsen et al. identify the following characteristics of a supply chain attack [53]:

1. Supply chain attacks can occur anywhere in the supply chain, and to any hardware or software in it, regardless of origin.
2. The attacks can be of any kind.
3. The goal of the attacks must be more than to breach a given system.

However, as discussed, both SCRM and C-SCRM utilize a broad approach that evaluates the risks of a wider range of events [43, 56]. This method of accounting for any type of incident or risk within a domain is called the *all-hazard approach* [62]. To maintain this holistic viewpoint and adhere to the all-hazard approach throughout this research, we will regard *cybersecurity risks throughout the supply chain* as: "the potential for harm or compromise that may arise from suppliers, their supply chains, their products, or their services. Cybersecurity risks throughout the supply chain are the results of threats that exploit vulnerabilities or exposures within products and services that traverse the supply chain or threats that exploit vulnerabilities or exposures within the supply chain itself" [13]. Given this definition Cyber Supply Chain Risk Management (C-SCRM) will be regarded as the management of these risks.

3.2 Academic literature background

This section presents the fundamental insights on the topic of C-SCRM, gathered from academic literature review as outlined in Section 2.1.2. These insights are categorized as identified challenges, risks and sources of risks. With these categories we aim to establish a clear understanding of the current landscape of C-SCRM and provide essential context for the development of our best practice implementation guideline.

3.2.1 Challenges

The academic literature reveals several significant challenges in effectively implementing and managing C-SCRM. These challenges span technical, organizational, and strategic dimensions, highlighting the multifaceted nature of modern supply chains.

Figure 3.1 shows an overview of the challenges that we identified in the literature. These challenges are structured into themes and subthemes. The figure maps these themes and subthemes to the articles included in our literature review. In the following sections, we discuss each of the themes and the specific insights within these themes gathered from the literature.

Lack of holistic and integrated approaches

As shown in Figure 3.1 one of the primary challenges in C-SCRM, identified in the literature, is the absence of holistic and integrated approaches. Many organizations address cybersecurity at a single-firm or even per department level [18, 23, 34, 47]. In these siloed approaches, there is often a primary focus on technical aspects, while neglecting the broader inter-organizational nature of supply chains [18, 5, 23]. This piecemeal approach overlooks the systemic nature of cyber risks, which can propagate across multiple tiers of the supply chain [79].

Cheung et al. [17] calls for more practical and integrated solutions to help organizations implement the measures developed in academia, stepping away from conceptual frameworks. Colicchia et al. [18] identified that C-SCRM initiatives are mainly adopted to 'respond' and 'recover', lacking a proactive approach for long-term capacity to adapt to changes. Mitigating this problem, Ghadge et al. [36] proposes

Category	Theme	Subtheme	Colicchia et al.	Ghadge et al.	Zheng and Albert	Alanazi and Solangi	Redondo et al.	Windelberg	Estay and Khan	Boyson	Creazza et al.	Gani et al.	Jarainy et al.	Collier and Sarkis	Pandey et al.	Eggers	Abrahams et al.	Hamm et al.	Sindhuja and Kunnathur	Adenekan et al.	Cheung et al.	Sobb et al.	Total
Challenges	Lack of holistic and integrated approaches		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	20
	Supply chain complexity and lack of visibility		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	20
	Difficulties in assessing and quantifying cyber risks				x	x	x		x	x	x		x		x	x	x	x	x	x	x	x	15
	Challenges in collaboration with suppliers	Inadequate due diligence			x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	17
		Lack of contractual oversight	x			x	x	x		x	x			x			x			x			9
		Limited monitoring capabilities	x	x		x	x		x	x		x	x		x	x	x		x	x	x		14
	Human and behavioral factors		x	x	x				x	x	x	x	x		x		x		x	x	x		13
	Dynamic and evolving threat landscape		x	x			x		x	x	x	x	x		x	x	x		x		x	x	14
	Resource constraints and lack of investment		x	x	x			x		x			x	x					x	x			9
	Regulatory and compliance complexity									x			x				x		x				4
	Lack of standardized policies and frameworks			x	x	x	x	x			x	x			x				x			x	10
		Total	7	7	7	7	8	6	7	10	8	7	9	5	8	6	9	3	10	8	7	6	

Figure 3.1: Comprehensive mapping of identified themes and subthemes within the category of challenges, linked to their respective academic sources.

the inclusion of the whole attack cycle, implementing pre-, trans- and post-attack strategies. Zheng and Albert [82] stresses the need for a holistic approach in the form of a systematic and cost-effective process to reduce risks throughout the entire supplier lifecycle, not just during acquisition. This also means adopting strategies for vendor off-boarding [1].

Furthermore, there is a lack of integration between supply chain risk management and cyber risk management [5]. Holistic approaches should integrate both domains and explore their intersection [70].

Windelberg [79] stresses that organizations need to consider the interplay of supply chain risk management objectives (security, reliability, safety, quality, and trustworthiness) rather than addressing them in isolation. These gaps highlight the need for a unified framework that encompasses the entire organization and multiple tiers of the supply chain while considering both technical and organizational factors.

Supply chain complexity and lack of visibility

The increasing complexity of modern supply chains presents a substantial challenge to effective C-SCRM [26, 41]. Supply chains are transforming from linear structures to complex, dynamic, and interconnected webs [19, 70]. Globalized supply chains often involve multiple tiers of suppliers, each with their own cybersecurity vulnerabilities [15, 36, 18, 79]. Alanazi and Solangi [5] discuss three dimensions of complexity in supply chains: the number of suppliers (horizontal complexity), divisions (vertical complexity), and geographical spread (spatial complexity).

These levels of complexity form a network of interconnected risks, where breaches can have cascading effects throughout the chain [82]. This is highlighted by Estay and Khan [26], stating that as supply chain complexity increases, interaction failures become more prevalent, making the traditional approaches focusing on individual components less effective.

As shown in Appendix C a great hurdle identified by all analyzed articles is the lack of visibility throughout the supply chain, resulting from the described supply chain complexity. Many organizations have limited insight into the different layers of the supply chain network to which they are connected, and the

cybersecurity practices of these different suppliers [36]. Most organizations do not have visibility beyond their first-tier suppliers [79, 15, 25].

This lack of transparency not only makes it difficult to assess and mitigate risks effectively but also hinders adequate action during and after an attack [47]. The dynamic nature of these networks also makes it challenging to keep track of all partners and provide a nurturing environment for collaboration [18].

Difficulties in assessing and quantifying cyber risks

Another challenge is the difficulty in assessing and quantifying cyber risks within supply chains. Traditional risk management approaches, often based on the assessment of probability and impact, are increasingly inadequate due to the difficulty of accurately estimating impacts in complex supply chains [23]. Since cyber risks originate from various sources, manifest in diverse forms, and differ significantly in their impact severity, it makes them challenging to asses and analyze [82, 47]. This hinders effective risk prioritization and mitigation [15]. These threats are constantly evolving, and the methods used to measure them need to be updated frequently as well. There is a need for a standardized approach that accounts for varying levels of supply chain risks across different contexts and industries [5]. Furthermore, the absence of real-world cybersecurity data in supply chain management makes it hard to create empirical models [82, 17]. Lack of shared data is often due to privacy concerns, reputation damage, and the lack of trust among supply chain partners [66]. Some research suggest quantified methods for assessing and ranking both risks and supply chain partners [82, 66]. However, these methods can be too encumbering for smaller organizations to implement [82].

Challenges in collaboration with suppliers

Reliance on third-party suppliers introduces a significant source of vulnerability in C-SCRM [36]. These third parties often have varying levels of security maturity, making them potential entry points for cyber attacks [70]. Managing these risks involves several challenges. First, there is **inadequate due diligence** where organizations fail to vet suppliers' security practices sufficiently [5]. A prominent cause for this is implicit trust assumptions between organizations, often without proper documentation or evaluation of risk factors [79]. This can lead to the incorporation of vulnerable components into the supply chain [19]. Weak points and new attack vectors are potentially introduced, while risks are not fully considered [82]. Collier and Sarkis [19] proposes the adoption of a zero-trust approach to prevent these assumptions from taking root. However, trust between suppliers and buyers increases efficiency by decreasing red tape in decision making [19]. Some level of trust is also needed between supply chain partners to facilitate information sharing without hindrance by security or competition concerns [47].

Since there is inadequate risk inventorization, organizations often fail to establish clear contractual requirements for cybersecurity with their suppliers [18]. This can cause a **lack of contractual oversight** [18]. When there are no legal agreements and responsibilities set, communication and collaboration between partners becomes harder [5, 1]. While effective collaboration and information sharing with suppliers are crucial for managing cyber risks [26] participants across the supply chain have "different understandings of risk management objectives and have varying capabilities for defining requirements and managing supply chain risk" [79]. Suppliers can start making risk trade-offs that benefit themselves, but not the acquirers further down the chain [79]. Contractual agreements can include requirements about incident reporting and knowledge sharing in order to streamline collaboration [23].

With no risk inventory and no requirement agreement there will be **limited monitoring capabilities** available [66]. Organizations lack the means to continuously monitor the ongoing security posture of their third-party suppliers [5]. Redondo et al. [66] propose the use of a threat intelligence system (TIS) and forecasting models to enhance monitoring capabilities. While regular monitoring is needed, such an extensive and quantified system is too encumbering for most organizations who lack the funding and knowledge to implement this effectively [82]. Other research opts for a more lightweight approach emphasizing data exchange and information sharing [47]. Abrahams et al. [1] highlights the need for continuous monitoring, including vendor performance, cybersecurity measures, and financial practices. These articles emphasize the need for robust procedures for the regular monitoring of suppliers to notice new risks as soon as possible.

Human and behavioral factors

The human element is also indicated as a critical factor in C-SCRM, with Sindhuja and Kunnathur [69] noting that humans are the weakest link in supply chains. Many cyber incidents result from employee negligence, lack of awareness, or malicious actions [82]. C-SCRM methods often feature a bias favoring technical risks, while behavioral risks are overlooked [36, 18]. The lack of adequate training and awareness among employees regarding security risks increases the likelihood of human error and vulnerabilities [58]. Addressing these risks requires a coordinated effort to raise cybersecurity awareness and nurture a culture of security within the organization and its supply chain [36, 34, 47, 3]. A dedicated governance team is required for setting the security tone and driving initiatives [34].

Dynamic and evolving threat landscape

The cyber threat landscape is constantly changing, with new threats and attack vectors emerging regularly [82]. The sophistication of cyber-attacks is increasing, requiring more complex and advanced defense mechanisms [34, 26, 3]. Where early attacks focused on single execution of simpler methods such as phishing and malware [36], modern attacks are much more complex, involving long-term campaigns [23, 25]. In addition, attackers are no longer solely targeting individual organizations. There is a clear trend towards targeting vulnerabilities in the supply chain [58, 25, 70]. Compromising a weaker link in the supply chain can provide access to the entire network, including larger, and more valuable targets [23]. This evolving threat landscape is difficult to manage [15, 25]. Therefore, organizations must continuously adapt their security strategies to mitigate new threats while staying informed about the latest attack trends, vulnerabilities, and security technologies [26, 15, 47, 58, 1].

Resource constraints and lack of investment

A further challenge lies in the allocation of resources to C-SCRM. Many organizations, particularly SMEs, lack the financial and technical capacity to implement robust cybersecurity measures [82, 47]. These resource constraints can lead to a situation where cyber risks are not effectively managed [79]. This lack of investment often stems from the perception that security is a cost center rather than an enabler of other business objectives and operational performance [36]. Security programs often need to compete with other internal initiatives for funding [19]. It becomes challenging to demonstrate a return on investment [69], as benefits are often measured in terms of avoided costs rather than increased profits [19].

Regulatory and compliance complexity

Organizations also face challenges in navigating the complex web of cybersecurity regulations and compliance standards [15, 47]. Different countries and industries have varying legal requirements for data protection and information security, which can be difficult for multinational organizations to adhere to [69]. Sometimes organizations even face conflicting regulations, leading to problems in implementation and prioritization of controls [15]. Suppliers asked to comply with security mandates can delay compliance, create a false pretense of compliance, or even leave the supply chain entirely [47]. This creates challenges when organizations try to maintain secure and reliant supply chains Staying on top of these regulations and ensuring compliance requires a robust framework and ongoing monitoring [1].

Lack of standardized policies and frameworks

The absence of standardized policies, protocols, and frameworks for C-SCRM adds to the complexity of the problems organizations face [79, 66]. Organizations often struggle to implement effective security measures due to a lack of guidance and consistent approaches [5]. Managerial capabilities fall short when trying to gain clear view of available standards and practices and implementing them [34]. The literature calls for industry-wide standards and collaborative strategies to ensure a baseline of cybersecurity across supply chains [36]. These standards should remedy the inconsistencies and inadequacies in current practices [58] and improve communication and collaboration for incident management [69].

3.2.2 Supply chain risks

To understand the measures needed to facilitate sufficient C-SCRM, it is paramount to understand the current risks that supply chains face. The following paragraphs summarize the multitude of risks

identified in the articles from our literature review.

Category	Theme	Subtheme	Colicchia et al.	Ghadge et al.	Zheng and Albert	Alanazi and Solangi	Redondo et al.	Windolberg	Estay and Khan	Boyson	Creazza et al.	Gani et al.	Jazairy et al.	Collier and Sarkis	Pandey et al.	Eggers	Abrahams et al.	Hammi et al.	Sindhuja and Kunnathur	Adenekan et al.	Cheung et al.	Solib et al.	Total
Supply chain risks	Data breaches and information security incidents		x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x	19
	Cyber-attacks	Malware infections	x	x	x		x	x		x	x	x		x	x	x	x	x	x	x	x	x	17
		Ransomware attacks		x							x	x			x			x		x	x	x	8
		Phishing attacks	x	x		x									x			x					5
		Advanced Persistent Threats (APTs)	x		x											x		x		x		x	6
		Distributed Denial-of-Service (DDoS) attacks		x												x		x				x	4
		Man-in-the-Middle (MITM) attacks																x			x		2
	Supply chain disruptions	Unavailability of critical services	x		x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	18
		Counterfeit products	x	x	x			x		x			x	x	x	x		x		x	x		12
		Tampering, theft and sabotage	x	x	x	x		x		x		x	x	x	x	x		x			x	x	14
		Total	7	7	6	4	3	5	2	5	4	5	4	5	7	6	2	10	3	6	7	7	

Figure 3.2: Comprehensive mapping of identified themes and subthemes within the category of challenges, linked to their respective academic sources.

Figure 3.2 shows an overview of the supply chain risks identified from the literature. These risks are structured into themes and subthemes. The figure maps the subthemes to the articles analyzed in our literature review, showcasing where information on these themes is gathered from. The next sections will discuss each of the themes and the specific insights within these themes gathered from the literature.

Data breaches and information security incidents

Colicchia et al. [18] reports that data breaches are perceived as one of the most disruptive risks for some organizations. Given that 19% of data breaches originate from compromised business partners, there is a growing need to mitigate the vulnerability of supply chains to information security incidents [47]. For example, compromise of customer or employee records can severely damage an organization's reputation and erode customer trust [36, 58]. Information leakage, whether intentional or unintentional, poses a risk to confidentiality and competitive advantage [34]. Poor security controls within any organization can lead to a data breach that affects the entire interconnected supply chain [34].

Cyber attacks

Cyber attacks represent a broader category of risks that target various components of the supply chain. These attacks can manifest in different forms; some broader types of attacks are identified in the literature. Colicchia et al. [18] for example, mention the proliferation of **Malware infections**, **Phishing attacks**, and **Advanced Persistent Threats (APTs)**. The latter are sophisticated long-term attacks aimed at gaining prolonged access to systems and data, requiring measures that are robust to the actions of adaptive adversaries [82]. **Distributed Denial-of-Service (DDoS) attacks** overwhelm systems with traffic, sometimes rendering even the most critical services unavailable to legitimate users [36, 25]. Communication channels in the supply chain can also be the target of cyber attacks, with **Man-in-the-Middle (MITM) attacks** interfering in communication streams by impersonating authentic actors [41]. Communication data can be intercepted and even altered without the knowledge of supply chain partners [17]. Cyber attacks can target various points in the supply chain, including ERP systems, company websites, and network infrastructure [23].

Supply chain disruptions

Disruptions to the supply chain reduce the reliability of services [47]. One disruption in a single firm can have a ripple effect through the supply chain leading to widespread disruptions [47]. These disruptions can take various forms. One of the risks with the greatest perceived impact is the **unavailability of critical services** [18]. These are incidents that disable critical infrastructure or essential service providers, which can disrupt the flow of goods and services [36, 82]. These disruptions can have far reaching effect when a focal company within a supply chain network becomes unavailable, deteriorating the entire chain and disrupting processes within other organizations [66]. Furthermore, disruptions can cause malicious actors to gain access to data, systems, products, or components. This can lead to **tampering, theft and sabotage**, altering them or making them unavailable, disrupting processes [36, 82, 19]. For example, hardware components can be supplied with pre-installed malware compromising any systems in which they are installed [58]. Windelberg [79] explicitly mentions the risks surrounding authenticity, in other words, the risks of **counterfeiting**. This includes "used or recycled components being sold as new, cloned items represented as being from the original manufacturer or unauthorized copies of software produced by an unauthorized supplier" [79]. Counterfeit goods infiltrating the supply chain can pose significant safety and health hazards, for example, when harmful contaminants are introduced into food or pharmaceuticals [19].

3.2.3 Sources of risks

It is valuable to know the sources of the identified sources of risks in order to develop effective mitigation measures.

Category	Theme	Subtheme	Colicchia et al.	Ghadge et al.	Zheng and Albert	Alamri and Solangi	Redondo et al.	Windelberg	Estay and Khan	Boyson	Creazza et al.	Gani et al.	Jazairy et al.	Collier and Sarkis	Pandey et al.	Eggers	Abrahams et al.	Hammi et al.	Sindhuja and Kunnathur	Adenekan et al.	Cheung et al.	Robb et al.	Total
Sources of risks	Internal sources	Current and former employees	x	x	x	x	x		x	x	x	x	x	x	x		x	x	x		x		16
		Internal technical problems	x	x				x		x	x	x	x		x	x	x	x			x	x	13
	External sources	Supply chain partners	x	x	x	x	x	x		x		x	x	x	x	x	x	x	x	x	x	x	19
		Malicious actors	x	x	x		x	x	x	x			x	x	x		x	x	x	x	x	x	16
		Natural disasters:	x	x	x		x										x					x	6
	Vulnerabilities in digital infrastructure	IoT device vulnerabilities		x								x			x	x		x		x	x	x	8
		SCADA system vulnerabilities													x	x		x			x	x	5
		Cloud vulnerability		x			x	x		x		x			x			x	x			x	6
		Insecure software		x			x	x		x		x	x	x	x	x	x	x	x	x			14
		Total	5	8	4	2	5	4	2	5	2	6	5	4	8	5	6	8	5	4	7	7	

Figure 3.3: Comprehensive mapping of identified themes and subthemes within the category of sources of C-SCRM risks, linked to their respective academic sources.

Figure 3.3 shows an overview of the sources of supply chain risks identified in the literature. These sources of risks are structured into themes and subthemes. The figure maps the subthemes to the articles analyzed in our literature review, showcasing where information on these themes is gathered from. The next sections will discuss each of the themes and the specific insights within these themes gathered from the literature.

Internal sources

Internal sources of cyber risks originate from within the organization. **Current and former employees** are increasingly becoming vehicles for malicious attacks [36, 18, 5]. This can be unintentional or intentional [36]. Intentional malicious behavior can be due to various motivations, including financial gain, revenge, or ideological reasons [36, 18]. Unintentional threats can arise from human error, negligence, or a lack of awareness regarding cybersecurity best practices [36, 82].

Apart from these insider threats we also identified **internal technical problems** as a indicated source of threats. Technical problems to the IT infrastructure can be internal factors to an organization "causing failures that compromise the operations and the flow of information across multiple tiers" [18]. These can also take the form of unsecured communication channels [18], outdated firewalls, [36], breakdowns [34], system misconfigurations [1], hardcoded credentials [41], reliance on outdated systems [70], and internal power outages [23]. Most of these are the result of non-deliberate actions and internal faults [79].

External sources

External sources of cyber risks originate outside the organization. The main risk vectors are the **supply chain partners** [1]. This includes suppliers and customers, who can introduce vulnerabilities into the supply chain or compromise the process of sharing and transmitting information and data [23, 18]. Supply chain partners are increasingly the primary target of cyberattacks [15]. Attackers target contractors and subcontractors in the supply chain due to their perceived vulnerability and access to valuable intellectual property [58]. This becomes increasingly difficult to detect when it involves suppliers beyond the first tier in the supply chain [58]. These attacks often aim to gain access to sensitive information of larger companies by targeting their supply chain partners [15]. This illustrates why, despite the long-standing relationship with supply chain partners, they should not be inherently trusted [19]. The interaction points of these partners are the most vulnerable to cyberattacks [36, 18, 82].

These points are exploited by **malicious actors** such as industrial espionage agents, foreign nation states, and hackers/hacktivists [41]. This illustrates how poor controls in one organization can make the supply chain as weak as the weakest member [34]. Critical infrastructures are especially facing a growing number of malicious actors that become increasingly sophisticated due to state-sponsored actors targeting them [25, 3]. This increases the resources and time that these malicious actors have to achieve their goals [3].

Lastly, **natural disasters** are identified as a source of risks and risks. Incidents caused by natural events can render systems out of service, leading to disruption of operational processes [23]. The mitigation and recovery of such events can be long [70]. If key suppliers are hit by these types of events, other organizations downstream of the supply chain will also experience problems [66].

Vulnerabilities in digital infrastructure

The increasing reliance on digital technologies introduces vulnerabilities that can be introduced internally or externally [36]. Integration of **IoT devices** into supply chain processes introduces new attack vectors, as these devices are often poorly secured [36, 41] and come with ubiquitous internet connections [70].

Similarly, **Supervisory Control and Data Acquisition (SCADA) systems** are prone to comparable vulnerabilities [58, 41]. This is due to their long lifespans, minimal maintenance, and lack of focus on network protection [70]. Incidents in these systems can cause entire industrial plants to malfunction or physically damage them [58, 25].

With the outsourcing of servers to **cloud platforms**, which reduces direct costs, organizations endure a loss of control over security, which may increase long-term indirect costs[36]. These services are prone to service stability issues, memory allocation errors, network connectivity problems, and DDoS attacks [70]. Gani et al. [34] identified IoT sensor compromise and mismanagement of cloud access as one of the most worrying cybersecurity issues for manufacturing firms, an industry that is highly dependent on these technologies.

Furthermore, **insecure software** can introduce vulnerabilities through poor development practices that can be exploited to gain unauthorized access to systems and data [36]. However, in the context of supply chains this problem becomes even more likely since there is an unwarranted trust between organizations, where software is regarded as safe by default because it comes from a legitimate source [66]. Software can then become insecure due to the introduction of malicious software updates by supply chain partners [19]. Development, build, or programming software can also become compromised, corrupting the device under development [25]. Insecure software can also be a result of internal actions, with employees introducing vulnerabilities due to non-malicious actions such as not installing patches when they are not critical or interfere with existing systems [79].

3.2.4 Measures from academic literature

The analyzed set of research articles does not offer extensive guidance on the implementation of security measures for C-SCRM. However, we did identify separate measures and common themes proposed in these articles. These are used to shape and prioritize our best-practices implementation guideline.

Category	Theme	Subtheme	Colicchia et al.	Ghadge et al.	Zheng and Albert	Alanazi and Solang	Redondo et al.	Wendelberg	Estay and Khan	Boyson	Creazza et al.	Gani et al.	Jazairy et al.	Collier and Sarkis	Pandey et al.	Eggers	Abrahams et al.	Hammi et al.	Sindhuja and Kunnathur	Adenekan et al.	Cheung et al.	Sobb et al.	Total
C-SCRM measures	Risk management and assessment	Risk/vulnerability identification	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	20
		Risk assessment	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	20
		Risk prioritization	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	20
		Continuous risk assessment and management		x		x			x	x				x	x		x		x	x	x		10
		Threat modeling and war gaming								x							x						2
	Security governance and strategy	Executive risk governance								x	x	x						x					4
		Information security strategy	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	20
		Multi-organizational security strategy	x	x		x					x				x			x	x				7
		Alignment with business goals	x	x		x					x				x			x					6
	Supply chain collaboration and integration	Supplier due diligence				x		x		x				x		x	x		x	x			8
		Supplier audits		x				x		x	x	x		x	x	x	x	x	x				11
		Contractual oversight				x		x		x				x			x			x			6
		Information sharing		x		x					x	x	x		x	x	x		x		x	x	11
		Joint risk assessments		x		x					x	x					x		x		x		7
		Collaborative recovery plan process	x	x		x			x	x	x	x	x		x	x	x	x	x		x	x	15
		Communication procedures with involved supply chain partners		x		x					x			x	x		x	x	x			x	9
	Security technologies and tools	Access control mechanisms		x				x			x	x		x		x	x	x	x	x	x		11
		Network security controls									x								x		x	x	4
		Data protection measures	x								x	x			x	x	x				x		7
		Software assurance tools						x		x					x					x			4
		Blockchain technology												x				x		x	x		4
		AI and machine learning																		x	x	x	3
	Operational security practices	Incident response planning	x	x	x	x			x	x	x	x	x		x	x	x	x	x		x	x	16
		Business continuity and disaster recovery planning									x						x						2
		Employee training and awareness	x	x						x	x				x		x		x	x	x		9
		Secure software development practices						x		x					x					x			4
		Physical security controls						x				x			x								3
	Continuous improvement and monitoring	Continuous monitoring				x								x	x		x			x	x		6
		Post-event reviews				x											x						2
		Regular security audits		x						x	x	x		x	x	x	x	x		x			11
		Continuous improvement processes				x				x				x	x								6
		Total	10	16	5	17	4	11	7	17	19	14	7	14	20	12	21	14	16	15	17	10	

Figure 3.4: Comprehensive mapping of identified themes and subthemes within the category of C-SCRM measures, linked to their respective academic sources.

Figure 3.4 shows an overview of the C-SCRM measures identified in the literature. These measures are structured into themes and subthemes. The figure maps the subthemes to the articles analyzed in our literature review, showcasing where information on these themes is gathered from. The next sections will discuss each of the themes and the specific insights within these themes gathered from the literature.

Risk management and assessment

The continuous process of identifying, analyzing, evaluating, and prioritizing cyber risks within the supply chain forms the foundation of a proactive C-SCRM strategy [17]. This proactive approach

enables organizations to anticipate potential threats and allocate resources effectively. This includes **risk/vulnerability identification** [17], pinpointing potential cyber threats and vulnerabilities across the supply chain. This can be done utilizing various techniques such as risk identification software [36], attack path analysis [82, 17], and Bayesian analysis [17]. Next comes **risk assessment** where likelihood and potential impact of identified risks are evaluated [15]. Suggested methods for this involve probabilistic approaches (e.g., Monte Carlo simulations), risk scoring, and the use of probability and impact matrices [15, 58]. To rank risks based on their potential impact and likelihood **risk prioritization** is needed to guide mitigation efforts towards the most critical threats [15]. Some research suggests expanding these practices into an ongoing nature of risk management, requiring regular reassessments, updates, and adaptations to the evolving threat landscape through **continuous risk assessment and management** [3]. To simulate potential attacks and identify additional vulnerabilities to design resilient systems and protocols, methods like **threat modeling and war gaming** are proposed [15].

Security governance and strategy

This category focuses on establishing the overall framework, policies, and organizational structures for managing cyber supply chain risks. It ensures that C-SCRM is aligned with business objectives and receives appropriate executive oversight. This involves **executive risk governance**, establishing an executive-level oversight body (e.g., a risk council) to guide C-SCRM strategy, set objectives, and ensure enterprise-wide alignment [15]. Furthermore, it is necessary to create a clear **information security strategy** [23]. Integrating IT, organizational, and supply chain security systems [36]. In addition, this security strategy should be shared as a **multi-organizational security strategy** across the supply chain to ensure consistent practices and coordinated responses [69]. These strategies should integrate the C-SCRM objectives with the overall business priorities to ensure **alignment with business goals** and security investments [5].

Supply chain collaboration and integration

Collaboration and information sharing among supply chain partners is noted as an important aspect of C-SCRM [23]. It is recognized that cybersecurity is a shared responsibility and requires coordinated efforts across the entire supply chain network [23]. To facilitate this, adequate **supplier due diligence** is needed [23], conducting thorough background checks, security reviews, and assessments of suppliers before onboarding and throughout the relationship [5]. This prevents untrustworthy partners from entering the supply chain, eliminating trust assumptions [79]. Established relationships should involve regular **supplier audits** to ensure compliance with established standards and identify potential vulnerabilities [1]. **Information sharing** involves sharing threat intelligence, security best practices, and incident information with supply chain partners to improve collective awareness and response capabilities [23]. **Joint risk assessments** are used to identify and address shared vulnerabilities, better coordinating responses to incidents [23]. Following these risk assessments it is recommended to create a **collaborative recovery plan process**, establishing clear procedures for communication, course of action and responsibilities during recovery and restoration phases [17]. Communication on these topics should be facilitated though secure **communication procedures with involved supply chain partners** [23, 70]. Establishing clear communication protocols with supply chain partners for collaboration and incident management is crucial in critical phases [23]. All of these controls should come with **contractual oversight**. Incorporating security risk management into contracts with suppliers [15].

Security technologies and tools

Technical solutions and tools are necessary to prevent, detect, and respond to cyber threats. The literature discusses a wide range of technologies, from basic security controls to advanced analytics and automation. A prominent technological measure discussed in the literature is implementing robust **access control mechanisms**, including encryption, multi-factor authentication, role-based access controls, strong password policies, and biometric authentication [19]. Basic **network security controls** are recommended as well, including installing and maintaining secure firewalls and gateways [17], cryptography [70], Intrusion Prevention Systems (IPS) [23], antivirus applications [69], digital signatures [69], and data and URL filtering [23]. This can be extended with maintaining accurate records of personnel handling sensitive data, keeping multiple data backups, and distributing data centers geographically [23]. These **data protection measures** together protect data integrity, confidentiality, and availability [58]. Using **software assurance tools** ensures third-party software integrity and authenticity [58] through

code audits to detect malware and viruses [15], the use of embedded signatures and certificates of conformance [15], independent validation and verification testing [79]. A more complex solution proposed in the literature involves **blockchain technology** to enhance traceability, immutability, data integrity, data sharing, data availability, and scalability [19]. Blockchain could primarily be utilized to provide a tamper-proof method for logging transactions throughout the supply chain, enhancing transparency [3]. To automate anomaly detections or filtering though monitoring data produced by other technological measures **AI and machine learning** are highlighted for their real-time threat detection capabilities, analyzing vast amounts of data to identify malicious activity [3].

Operational security practices

This category encompasses the day-to-day activities and procedures that organizations implement to maintain a secure operating environment. It focuses on embedding security into all aspects of operations. For this, providing regular security awareness training to employees to reduce the risk of human error and promote a security-conscious culture is paramount [18]. **Employee training and awareness** educates employees about the risks associated with third-party relationships and their role in managing these risks. This includes training on identifying potential risks, reporting mechanisms, and the importance of security awareness [1]. Furthermore, **physical security controls** protect facilities, data centers, products, and other critical assets by limiting access from unauthorized access and environmental dangers [34]. On the other hand, **secure software development practices** should take supply chain risks into account as well through code reviews, automated testing, and vulnerability assessments covering third-party software implemented in systems [3]. Finally, organizations should plan for disruption of their day-to-day processes through **incident response planning**, creating coordinated courses of action to address and manage a security breach or cyberattack [15]. This is followed by **business continuity and disaster recovery planning** including evaluating vendors' continuity capabilities and developing robust transition strategies, exit strategies and data migration plans, to maintain operations during disruptions [1].

Continuous improvement and monitoring

The ongoing nature of C-SCRM requires continuous monitoring, evaluation, and improvement. It ensures that C-SCRM strategies remain effective in the face of evolving threats. **Continuous monitoring** involves implementing systems for real-time monitoring and logging of activities, including material, information, and financial flows [19]. This also involves monitoring of third-party relationships, including vendor performance, cybersecurity measures, and financial practices [1]. **Regular security audits** can structure this approach both internally and externally. After incidents the literature recommends to conduct **post-event reviews** establishing feedback loops to create lessons learned to be shared through the supply chain [1]. The aforementioned measures are foundational to setup an adequate **continuous improvement process**, adapting security measures based on emerging threats vulnerabilities, and lessons learned [5].

3.3 Industry resources

In recent years, guidance on adequate C-SCRM processes has primarily been offered through government and industry institutions creating various types of standards, guidelines, and practices. This section provides a detailed overview of the key industry resources addressing C-SCRM that our implementation guideline builds on, highlighting the contributions of each document to this critical domain. By dissecting the contents and discussing the key aspects, we offer an understanding of the resources that are already available for organizations to increase their C-SCRM posture.

To create a holistic view of the commonalities and interrelationship of the key industry resources, we distill a set of best practices prevalent across all documents. This section further discusses each of the key industry resources, starting with the general outline of each document followed by the specific information and guidance it provides in the context of C-SCRM.

3.3.1 NIST IR 8276

NIST Interagency Report 8276 [12], titled "Key Practices in Cyber Supply Chain Risk Management: Observations from Industry", presents key practices and recommendations derived from research con-

ducted in 2015 and 2019, including expert interviews and analysis of existing resources. Published in February 2021, this document, unlike the more prescriptive NIST SP 800-161r1, offers a more practical, implementation-focused approach to C-SCRM for organizations of all sizes and complexities.

The document emphasizes the importance of integrating C-SCRM across the entire organization, establishing a formal program, understanding the organization's supply chain, collaborating closely with key suppliers, and it highlights the criticality of identifying, assessing, and mitigating cyber supply chain risks to ensure business resilience. It also highlights the need to include key suppliers in resilience and improvement activities and to assess and monitor supplier relationships throughout their lifecycle. The report consists of eight key practices and 24 key recommendations for how to put these practices into use. It concludes with providing references to other resources that provide more guidance on C-SCRM. Overall, the document aims to provide a starting point for organizations that need to begin addressing the challenge of C-SCRM offering a birds-eye view towards structuring an initial approach.

Provided guidance

NIST IR 8276 is structured around eight key practices that identify established and emerging practices that have been shown to be effective [12]:

1. Integrate C-SCRM across the organization
2. Establish a formal C-SCRM program
3. Know and manage critical components and suppliers
4. Understand the organization's supply chain
5. Closely collaborate with key suppliers
6. Include key suppliers in resilience and improvement activities
7. Assess and monitor throughout the supplier relationship
8. Plan for the full life cycle

Organized according to these key practices the document proposes a set of 24 key recommendations that outline how these practices can be implemented from a people, process, and technology perspective. Additionally, it provides a mapping between these 24 recommendations and several government and industry resources to guide its audience to other documentation that provides further guidance on the specific implementation of these recommendations. This mapping features three of the resources adopted in our own industry resource analysis (NIST SP 800-161r1 upd1 [13], ISO/IEC 27002 [45], and NIST.CSWP.02042020-1 [14])

The DORA RTS documents are not covered in this mapping. We expand on this mapping by adding both the DORA RTS 84 on ICT Risk Management Framework and DORA RTS 86 on ICT services supporting critical or important functions.

The supporting information for this new mapping, created in this research, is provided in Appendix A, which details the specific articles from both DORA RTS documents that offer guidance or recommendations for implementing this practice. Figure 3.5 illustrates the mapping created by NIST between the recommendations of NIST IR 8276 [12] and the selected industry resources, expanded with the original mapping to DORA RTS 84 and 86, thereby creating a comprehensive cross-reference between the NIST IR 8276 recommendations and the resources reviewed in our research.

Best practice	Industry resource:	NIST SP 800-161	NIST.CS WP.0204 2020-1	ISO/IEC 27002	DORA RTS 84	DORA RTS 86	Total
	Establish supply chain risk councils that include executives from across the organization (e.g., cyber, product security, procurement, ERM, business units, etc.)	✓	✓		✓		3
	Create explicit collaborative roles, structures, and processes for supply chain, cybersecurity, product security, and physical security functions		✓		✓	✓	3
	Increase board involvement in C-SCRM through regular risk discussions and sharing of measures of performance		✓		✓	✓	3
	Integrate cybersecurity considerations into system and product life cycles	✓	✓		✓	✓	4
	Clearly define roles and responsibilities for security aspects of specific supplier relationships	✓	✓	✓	✓	✓	5
	Use master requirements lists and SLAs to establish requirements with suppliers	✓	✓	✓	✓	✓	5
	Propagate security requirements to suppliers' sub-suppliers	✓	✓	✓			3
	Train key stakeholders in the organization and within the supplier's organization	✓	✓	✓			3
	Terminate supplier relationships with security in mind	✓		✓	✓		3
	Use Criticality Analysis Process Model or BIA to determine supplier criticality	✓	✓		✓	✓	4
	Establish visibility into suppliers' production processes to identify defect rates, causes of failure, and testing		✓		✓		2
	Know if the organization's data and infrastructure are accessible to suppliers' sub-suppliers	✓	✓	✓	✓		4
	Mentor and coach suppliers to improve their cybersecurity practices	✓	✓		✓		3
	Require use of the same standards within acquirer and supplier organizations		✓				1
	Use acquirer assessment questionnaires to influence acquirer cybersecurity requirements		✓				1
	Include key suppliers in IR, DR, and CP plans and tests	✓	✓	✓	✓	✓	5
	Maintain a watchlist of suppliers who had issues in the past and about which the acquirer should be cautious for future use (e.g., "Issue Suppliers"); such suppliers should only be used after approval from supply chain risk council		✓		✓	✓	3
	Establish remediation acceptance criteria for the identified risks	✓	✓	✓	✓	✓	5
	Establish cybersecurity requirements through Security Exhibit, Security Schedule, or Security Addendum document		✓		✓		2
	Establish protocols for vulnerability disclosure and incident notification	✓	✓	✓	✓	✓	5
	Establish protocols for communications with external stakeholders during incidents	✓	✓	✓	✓	✓	5
	Collaborate on lessons learned, and update joint plans based on lessons learned	✓	✓	✓	✓		4
	Use third-party assessments, site visits, and formal certification to assess critical suppliers	✓	✓	✓	✓		4
	Have plans in place for supplied product obsolescence	✓		✓	✓	✓	4
	Total	17	22	13	20	12	

Figure 3.5: Mapping between the recommendations of NIST IR 8276 and the documents included in our analysis. Sourced from Boyens et al. [12] (first 4 columns) and expanded with an additional mapping to DORA RTS 84 and 86 (last 2 columns).

3.3.2 NIST SP 800-161r1 upd1

The NIST Special Publication 800-161 Revision 1 [13], updated as of November 2024, provides a detailed framework for managing cybersecurity risks throughout the supply chain. This document addresses the risks associated with products and services that may contain malicious functionality, be counterfeit, or be vulnerable due to poor manufacturing and development practices. It emphasizes the importance of integrating C-SCRM into overall risk management activities by applying a multilevel approach. Key aspects include the development of C-SCRM strategy implementation plans, policies, and risk assessments for products and services.

NIST SP 800-161r1 upd1 addresses C-SCRM from three different perspectives: 1) the enterprise level, 2) the mission and business process level, and 3) the operational level. The document outlines specific stakeholders , responsibilities and controls across these three levels. In addition, it highlights a set of success factors forming the requisite enterprise processes in making C-SCRM successful. These span the processes of acquisition, information sharing, training and awareness, capability implementation measurement, and resource dedication. Furthermore, the document offers additional guidance on a

range of subjects by including appendices outlining multiple frameworks and templates. The publication aims to enhance the security, resilience, reliability, safety, integrity, and quality of products and services throughout the supply chain.

Provided guidance

NIST SP 800-161r1 frames C-SCRM as an enterprise-wide, team-based initiative. The guidance stresses that managing supply chain risks is "a complex undertaking that requires cultural transformation and a coordinated, multidisciplinary approach across an enterprise" [13]. In practice, this involves the establishment of dedicated C-SCRM teams under a shared responsibility model. These teams span the organization, combining cybersecurity, procurement, risk management, engineering, software development, legal, and human-resources experts, so that supply chain threats are viewed from all critical perspectives. NIST explicitly breaking down silos by chartering cross-functional councils of senior leaders with clear goals, authorities, and meeting cadences. These multidisciplinary groups ensure that C-SCRM activities such as strategic sourcing, contract requirements, and risk mitigation, draw on the full range of enterprise expertise.

Governance, strategy, and integration
The document calls for a formal governance framework that begins at the executive level. At Level 1 (enterprise), NIST directs organizations to define and approve a high-level C-SCRM strategy, implementation plan, and policy under executive sponsorship. These top-level documents establish the enterprise's risk management requirements, articulate its risk tolerance and priorities, and "set the tone, governance structure, and boundaries" for C-SCRM across the organization. Executive leaders are tasked with "form[ing] governance structures and operating model" [13] for C-SCRM and framing the enterprise-wide risk through, for example, setting the risk appetite. The guidance notes that the chosen governance model must explicitly define C-SCRM authority and accountability: for example, a centralized model may place a C-SCRM program office under executive oversight, whereas a decentralized model might delegate authority to operational units or departments.

NIST also prescribes an upfront "risk framing" activity: enterprise leadership must document assumptions about supply-chain threats, system constraints, regulatory requirements, and risk appetite that will guide all C-SCRM decisions. Once that context is established, the enterprise issues its C-SCRM policy, which formally "establishes the C-SCRM program's purpose, outlines the enterprise's C-SCRM responsibilities, [and] defines and grants authority to C-SCRM roles across the enterprise" [13]. NIST insists that all of these C-SCRM activities must be woven into existing risk management and system lifecycle processes. For example, organizations are told to integrate supply chain risk activities into their SDLC and to align C-SCRM risk assessments with the NIST Risk Management Framework and enterprise risk hierarchy.

Roles and responsibilities by level
The document systematically assigns roles and tasks at each level of the organization. At Level 1 (enterprise), the generic stakeholders are executive leaders who must "define Enterprise C-SCRM strategy", "form governance structures", and "frame risk for the enterprise" [13]. Their activities include approving the high-level implementation plan and policy, authorizing resources, and setting the enterprise risk appetite. At Level 2 (mission and business process), stakeholders include program/project managers, and other process owners. These mid-level managers are expected to develop mission-specific C-SCRM strategies and policies that reflect the enterprise guidance. NIST notes that Level 2 teams should "develop mission and business process-specific strategy", write the detailed policies and procedures, and "reduce vulnerabilities at the onset of new IT projects or related acquisitions" [13].

They also tailor the enterprise risk framework by setting risk tolerances for their processes and actively manage risk within their mission areas. Level 3 (operational) stakeholders are the engineers and practitioners who actually build and deploy systems. These teams are responsible for the detailed execution of C-the program, they "develop C-SCRM plans" [13], implement the policies and controls, and adapt the requirements to systems or components throughout the lifecycle.

Level 3 staff follows the constraints imposed by Levels 1 and 2 and provide feedback upward. NIST indicates that operational teams "report on C-SCRM to Level 2" [13], enabling the two-way flow of information. Across the levels, communication is emphasized: the multilevel process is intended to operate "with the overall objective of continuous improvement of the enterprise's risk-related activities" [13] through ongoing coordination.

Control families and implementation
NIST SP 800-161 integrates supply chain risk controls into the standard security control framework. It identifies relevant controls from NIST SP 800-53 Rev.5 [57] and organizes them into the same 20 security control families. This overlay approach allows organizations to leverage familiar assessment and tailoring processes. For each family, the publication adds supplemental guidance or new C-SCRM-specific controls as needed to address supply chain issues. During the risk management "Respond" step, agencies are instructed to select and tailor these C-SCRM controls at appropriate baselines (high, moderate, low) and apply them to mitigate identified supply chain risks. The clear mapping to SP 800-53 ensures that C-SCRM controls can be implemented internally or flowed down to contractors in a consistent fashion.

Templates and documentation
The NIST guidance also provides practical templates and examples for C-SCRM documentation. Appendix D of SP800-161 includes an illustrative C-SCRM Strategy and Implementation Plan template, a C-SCRM Policy template, and templates for system-level C-SCRM plans and risk assessments. These examples outline the sections and content that each document should contain. For instance, the strategy template lists as typical components the inclusion of enterprise-wide risk management requirements, ownership, risk tolerance, roles and responsibilities, and escalation criteria in the strategy and plan. It also provides sample text for Level 1 and Level 2 policy statements to ensure the policy's scope and objectives are clearly articulated. By following these templates, organizations can produce consistent, standardized C-SCRM plans, policies, and procedures that align across all tiers of the enterprise.

Metrics and continuous improvement
Finally, the publication calls for an iterative, metrics-driven program where feedback and measured results drive ongoing refinement of the C-SCRM framework. NIST SP 800-161 makes continuous improvement central to C-SCRM program management. It recommends that organizations define key performance metrics and actively track them to inform leadership and improve the program's effectiveness. For example, agencies should collect metrics on supply chain risk assessments, supplier performance, incident investigations, and other indicators of program maturity. Importantly, NIST urges the use of leading indicators to make C-SCRM more predictive: "apply insights gained from leading C-SCRM metrics [...] to shift from reactive to predictive C-SCRM strategies and plans" [13] as the threat landscape evolves. As C-SCRM capabilities mature, NIST also encourages adopting advanced practices such as automating C-SCRM workflows and using quantitative risk analysis to reduce uncertainty. All of these measures should demonstrate "reductions in risk exposure and improvements in the enterprise's security outcomes" [13].

3.3.3 ISO/IEC 27002

ISO/IEC 27002:2022 [45] is an international standard that provides specific controls for establishing, implementing, maintaining, and improving an Information Security Management System (ISMS) focused on cybersecurity. While not specifically focused on supply chain risk management, its principles and controls for information security are highly relevant to C-SCRM. The standard offers a wide range of security controls categorized into domains such as physical security, access control, cryptography, and security awareness. These controls can be adapted and applied to manage cybersecurity risks within an organization's supply chain. ISO/IEC 27002 serves as a practical blueprint for organizations aiming to safeguard their information assets against cyber threats. By following these guidelines, companies can proactively manage cybersecurity risks and protect critical information from unauthorized access and loss.

Provided guidance

ISO/IEC 27002:2022 emphasizes formal policies and procedures for managing supply-chain relationships and risks. It advises that organizations define topic-specific information security policies, including those addressing supply chain-related risks.

These policies should be formally approved, regularly reviewed, and aligned with business, legal, and regulatory requirements. ISO emphasizes the importance of explicitly covering supplier relationships in these policies, ensuring that supplier types are inventoried and assessed according to the sensitivity of the information they may access or process. Contracts and agreements with suppliers should clearly articulate security responsibilities, data handling obligations, and termination procedures, ensuring that security expectations persist throughout the lifecycle of the supplier relationship.

The standard further recommends periodic evaluation and monitoring of suppliers to verify compliance with agreed-upon security practices. This includes ensuring that outsourced services and third-party engagements are assessed not only at onboarding but continuously throughout the relationship.

People-based controls
Human factors are an essential part of ISO 27002's risk management framework, particularly in the context of third-party interactions. The standard mandates background screening, confidentiality agreements, and defined responsibilities for both internal staff and supplier personnel. These requirements should be formalized in contracts and supported by regular security awareness training programs.

Roles and responsibilities related to supplier engagement must be clearly allocated, documented, and communicated. The standard notes that personnel should be equipped with the necessary knowledge and skills to manage supplier risks, and organizations should ensure these competencies are kept up to date. ISO encourages organizations to define escalation paths and internal mechanisms (such as whistleblowing channels) for reporting supplier-related incidents or violations.

Physical controls
ISO 27002 prescribes a set of physical and environmental controls designed to protect information assets across locations, including off-premises and vendor-managed facilities. This includes ensuring secure transport and custody of equipment, proper storage conditions, and chain-of-custody documentation. Suppliers and third parties handling organizational assets must apply physical protections comparable to those within the primary organization's environment. Organizations are encouraged to establish contractual expectations and periodic audits to ensure that physical controls at supplier sites are maintained at the required security level. These measures protect sensitive data and critical hardware from theft, tampering, or unauthorized access, especially during transport, staging, or disposal phases.

Technical and development controls
ISO 27002 offers comprehensive guidance on technical controls that directly reinforce supply chain cybersecurity. The standard mandates segregation of development, test, and production environments to prevent unauthorized deployment of unverified software. Additionally, it calls for secure coding practices, rigorous access control, change management, and vulnerability management throughout the development lifecycle.

The standard requires defining deployment rules and authorizations for moving software into production, plus monitoring and logging any changes in the development. Asset management is another foundation: organizations should maintain an accurate inventory of hardware, software, and components (including vendor, version and deployment status) to support vulnerability management. Organizations are advised to use scanning tools, penetration testing and secure coding practices to detect malicious code or defects in third-party components. Access controls are also emphasized: the guidance notes that supplier access to organizational information must be controlled, via NDAs, encrypted channels or least-privilege credentials.

Incident response and monitoring
The standard mandates that organizations plan and prepare for security incidents by defining clear response processes, roles and communication channels in advance. In particular, it highlights coordination with external parties as part of incident handling. Organizations are advised to include incident notification and collaboration requirements in supplier contracts, and to regularly review logs and security reports from suppliers to detect anomalies.

Lifecycle Management
ISO 27002 recommends integrating supply chain controls from onboarding to offboarding. Contracts should outline not only operating requirements but also detailed termination procedures. including access revocation, data destruction, and asset return. Secure decommissioning of systems and formal closure of services helps minimize residual risks and ensures clean disengagement from supplier relationships. Lifecycle considerations extend to procurement, asset replacement, system upgrades, and compliance audits.

3.3.4 NIST.CSWP.02042020-1

This document, titled "Case Studies in Cyber Supply Chain Risk Management: Summary of Findings and Recommendations," [14] published by NIST in February 2020, summarizes findings from a series of case studies investigating the evolution of C-SCRM practices. The research involved interviews with 16

subject matter experts from six diverse companies across various industries. This report analyzes how C-SCRM practices have evolved since 2015, bringing to light current key practices.

It describes trends, correlations, and novel findings from an analysis of the case studies as a whole and offers recommendations for further research and guidance development. The document emphasizes the evolving nature of C-SCRM and the need for practical guidance and methods for implementing and evolving C-SCRM programs.

Provided guidance

The case studies reveal that mature C-SCRM programs exhibit close integration across functional and business lines, engaging executive leadership effectively. They highlight the importance of executive sponsorship for effective C-SCRM and the inclusion of executives from various departments in C-SCRM activities. It recommends to hold regular and scheduled update sessions where a relevant executive presents status reports, practitioner recommendations, challenges, and business impact assessments based on technical metrics. This enhances communication between business functions and creates an increasingly cyber-literate Board.

Multidisciplinary collaboration
The case studies exhibit that effective programs succeed by dismantling organizational silos and establishing working groups that include stakeholders from procurement, IT/security, engineering, legal, and other relevant departments. For example, many organizations facilitate collaboration between supply chain and cybersecurity teams through joint incident reviews and threat briefings. Some organizations assign embedded security roles within procurement or development teams to ensure that cybersecurity requirements are integrated early in sourcing decisions. This approach allows both technical and operational considerations to inform vendor engagement, while fostering shared understanding and accountability across departments. Establishing shared tools, templates, and communication routines further supports the exchange of information, ensuring risks are detected, evaluated, and addressed comprehensively.

Supplier risk identification and classification
The document showcases a wide range of methods used to identify and classify supplier risk. While some organizations rely on informal knowledge or ad hoc questionnaires, more advanced programs adopt structured approaches, including initial screenings and self-assessments to collect baseline risk indicators. The use of risk scoring systems allows organizations to assign criticality levels to suppliers based on business impact, access privileges, operational reliability, and strategic importance. These scores help prioritize resources and determine the intensity of oversight. More mature organizations benchmark supplier maturity using external standards like ISO/IEC 27001 or SOC 2 report, ensuring repeatable and defensible evaluations. Supplier risk classification is also built into contracting practices, where high-tier suppliers must meet stricter cybersecurity terms, including disclosure requirements, audit rights, and incident reporting obligations. Lower-tier suppliers may face lighter oversight, with contract clauses adapted to the assessed risk profile.

Supply chain integration and lifecycle management
According to the case studies, mature organizations conduct risk assessments early during product or service development, enabling proactive identification of single points of failure or vulnerabilities in component sourcing. Cybersecurity requirements are often defined up front and communicated via proposal requests and pre-engagement evaluations. Once suppliers are onboarded, continuous monitoring becomes essential to track compliance with service-level agreements, perform security audits, and assess vendor resilience in the face of evolving risks. Many organizations maintain centralized or hybrid governance structures that manage C-SCRM across business units. In blended models, a central office may set policy and approve vendor engagement decisions, while business units handle operational execution. Integrated governance ensures continuity of security controls from initial supplier selection through to maintenance and decommissioning.

Performance metrics and continuous improvement
The document indicates that most organizations currently lack formalized metrics, though they are working toward them. Some examples include tracking CVSS scores for vulnerabilities in supplier components or monitoring the percentage of suppliers achieving defined cybersecurity benchmarks. Industry frameworks such as the NIST Cybersecurity Framework or ISO standards serve as external benchmarks against which progress can be measured. Preventive controls, such as segmentation or intrusion detection systems, are increasingly adopted to proactively reduce risk. Organizations also invest in automation

tools for real-time monitoring of supply chain performance, alerting teams to disruptions or anomalies. Continuous supplier improvement is another emphasized area, with several case study participants reporting that clear communication, mentoring, and collaborative security assessments have helped elevate supplier security practices over time. By documenting improvement efforts and routinely analyzing outcomes, organizations can refine their strategies, create accountability, and maintain alignment with the evolving threat landscape.

3.3.5 DORA RTS

The Digital Operational Resilience Act (DORA) is a piece of regulation that aims to enhance the digital operational resilience of the EU financial sector. The Regulatory Technical Standards (RTS) under DORA provide detailed guidelines to ensure financial entities can effectively manage Information and Communication Technology (ICT) risks and third-party dependencies. The RTS provide details on inter alia the following key components:

- ICT risk management framework: This includes tools, methods, processes, and policies to harmonize ICT risk management across different financial sectors. It ensures entities can handle ICT-related risks effectively.
- Incident classification: Criteria for classifying major ICT-related incidents, including materiality thresholds and details for reporting significant cyber threats.
- ICT third-party service providers: Governance arrangements and risk management policies for financial entities using third-party ICT services, ensuring control over operational risks, information security, and business continuity.

The Dora RTS collection consists of 5 documents with more supplemental resources expected in the future. For this research, we have chosen to only include RTS 84 on ICT third-party service providers and RTS 86 on the ICT risk management framework, due to their higher relevance to C-SCRM compared to other RTS. RTS 86 focuses on the requirements for ICT risk management frameworks, emphasizing the need for robust strategies to identify, assess, and mitigate risks associated with ICT supply chains. RTS 84, on the other hand, provides detailed guidelines for managing ICT third-party risk, including the establishment of contractual agreements and continuous monitoring of third-party service providers. These standards offer practical and targeted approaches to C-SCRM, making them particularly valuable for our study on enhancing cybersecurity resilience through effective supply chain risk management practices.

Provided guidance from RTS 84

The RTS mandates a formal governance framework for third-party ICT risk. It requires the management body to adopt a written policy on the use of ICT services for critical or important functions and ensure it is implemented across the organization This policy must be reviewed at least annually and updated promptly as needed. Internally, the policy must clearly assign responsibility for approving, managing and documenting each relevant contract, and ensure that staff with appropriate skills and expertise are in place to oversee those arrangements. Senior management must remain fully accountable for third-party ICT risk and embed oversight roles and processes into the entity's governance structure.

Criticality assessment and risk evaluation The RTS stresses that entities must identify and evaluate critical services before contracting. The policy must define or reference a clear methodology for determining which ICT services support critical or important functions, and it must specify how often that determination is reviewed. Before entering any contract, the entity must conduct a comprehensive risk assessment. This assessment must consider all applicable regulatory requirements and all major risk categories. In particular, it should evaluate the impact of the third-party service on the entity's operational, legal, reputational and information-security risks, including risks to data confidentiality and integrity. The policy should explicitly address risks tied to data availability and location and ICT concentration risk.

Contractual safeguards The RTS requires several safeguards during the contracting process to protect critical functions. Key requirements include:

- Contracts must be in writing and include all provisions required by DORA Article 30.

- Contracts must grant rights to information access, inspection, audit and ICT security testing by the entity or its delegates.
- The entity should use rigorous audit and testing methods before entering into a contractual arrangement.
- provider-generated certificates or reports must be verified to over the entity's key systems and controls, are kept up to date, and meet accepted professional standards.
- Changes to an agreement must be formalized in writing: the policy requires that any amendments are documented, dated and signed by all parties, and that a clear renewal process is defined.

Subcontracting and data location The RTS requires entities to consider subcontractors and data residency in their due diligence. The acquirer must identify if the ICT service provider uses subcontractors to perform any part of a critical service. Likewise it must assess where data will be processed or stored: if data is handled in a third country, the entity must consider any additional operational, legal or sanctions-related risks.

Ongoing oversight and monitoring The RTS emphasizes that oversight must continue throughout the contract. It requires that contracts themselves specify measures and indicators for ongoing monitoring of the ICT service provider's performance. In support of this, the entity must establish concrete monitoring activities. For example, the entity should track key performance and risk indicators for the service, such as KPIs, control metrics, audit results or self-assessments. Furthermore, the provider must notify the entity promptly of any relevant ICT-related incidents or disruptions. If deficiencies are identified , the entity must ensure the provider takes timely corrective action. A policy should define how shortcomings trigger remediation measures and set deadlines to verify that fixes are implemented. All oversight results must be documented.

Exit strategy planning Finally, the RTS mandates that entities plan for termination of third-party services. The policy must include a documented exit plan for each critical ICT contract, which is reviewed and tested regularly. This plan should explicitly address scenarios such as provider failure, service interruptions or unexpected termination of the contract, ensuring that the entity can maintain or restore its critical functions. The exit plan must be realistic and feasible: it should be based on plausible risk scenarios, reasonable assumptions and should include an implementation schedule consistent with the contract's termination provisions.

Provided guidance from RTS 86

RTS 86 mandates that financial entities establish robust governance structures for ICT risk and supply chain management, with clear reporting to senior management. In particular, entities must furnish regular reports on ICT projects, especially those impacting critical or important functions, to the management body, with review frequency and detail scaled to project importance. ICT policies must explicitly define roles and responsibilities for security and risk activities. For example, roles for ICT security policy development and maintenance must be identified, and policies must be reviewed in line with regulatory obligations.

ICT risk management integration The RTS emphasizes integrating ICT risk management with broader business processes and strategies. For instance, it requires that testing of ICT business continuity plans take into account the entity's Business Impact Analysis (BIA) and formal ICT risk assessment. This links technical resilience plans to the organization's overall business continuity planning. Likewise, ICT policies must be adaptive: the RTS explicitly requires that entities consider material changes to their business operations, ICT environment or the cyber threat landscape when updating policies. By aligning ICT risk controls with enterprise strategy and anticipated changes, the guidance ensures that supply chain risks are addressed as part of the ongoing risk management framework.

Risk identification and classification Financial entities must comprehensively identify and classify all critical ICT assets and functions, including those delivered by third parties. All critical or important functions and their supporting information, ICT assets, and service providers must be identified, documented and classified. This includes recording the end-of-support dates for services provided by third-party vendors for each ICT asset.

Control implementation and monitoring The RTS provides detailed guidance on implementing and monitoring controls to manage supply chain and ICT risks. It highlights robust vulnerability and patch

management: entities must establish formal procedures for vulnerability scanning and timely deployment of patches. Financial entities are expected to perform regular automated scans of all ICT assets (at least weekly for those supporting critical functions) and require ICT third-party providers to address and report any vulnerabilities found. In addition, strong logging and network security measures are mandated. For example, the RTS stresses that logging of events related to access control, capacity, change management and network traffic "enhances monitoring capabilities," and that logging infrastructure must be protected against tampering. Encryption and secure network controls must align with industry best practices to ensure confidentiality, integrity and availability across connections.

Incident preparedness and recovery The RTS requires comprehensive incident management and recovery planning that explicitly includes supply chain scenarios. Financial entities must document an ICT incident management process and have policies covering detection, response and reporting of ICT incidents. Business continuity testing must simulate severe disruption scenarios. In particular, the guidance mandates that testing include failure scenarios involving ICT third-party providers, such as the insolvency or operational failure of a vendor. Response and recovery plans must specify activation/deactivation criteria and detail actions to restore critical systems supporting important functions.

Documentation and review Consistent documentation and periodic review of the ICT risk framework are mandated to capture lessons learned. The RTS reinforces the requirement (from DORA Article 6) that entities document their ICT risk management framework and review it regularly, with a full audit trail of changes. Entities must produce a formal report on each review's outcome, detailing updates to the framework and justifying any changes. Through these measures, entities create a cycle of continuous improvement and accountability in their ICT and supply chain risk governance, ensuring that policies evolve to meet emerging threats.

Chapter 4

Best practice implementation guideline

This chapter presents the complete best-practice implementation guideline developed through the research process outlined in Section 2.3. The guideline consists of 17 best practices, derived from a synthesis of academic literature, industry standards, and expert interviews. These practices are organized into four thematic categories: Governance, Strategies and Procedures, Monitoring and Assessment Methods, and Structured Risk Management.

Figure 4.1 provides a visual overview of how these best practices collectively form a coherent and actionable C-SCRM capability. Each numbered text item in the figure (e.g., 1.1, 2.4, 3.2) directly represents a specific best practice as described in detail within this chapter. The first digit refers to the category (e.g., "2" for Strategies and Procedures), while the second digit indicates the best practice's position within that category. Some best practices appear in multiple areas of the visual model, reflecting their cross-cutting relevance and influence on different C-SCRM activities.

Figure 4.1 uses boxes to represent major structural components of a C-SCRM function. Arrows and labeled connectors such as "includes," "establishes," and "results in" indicate the directional relationships between best practices and these structural components. For example best practice 1.4 establishes the C-SCRM policy which includes the best practices from the "Strategies and Procedures" category. These relationships are also explicitly discussed in this chapter where relevant, to explain how specific practices contribute to the formation of supporting artifacts, contractual measures, or daily risk management routines.

The implementation process begins (in the upper left corner of the demonstrator) with establishing a governance structure, which serves as the foundational layer for subsequent efforts. Governance practices enable the rollout of the core Strategies and Procedures, which cover implementation activities such as secure development, contracting, training, and incident response planning. These practices, in turn, inform the operational mechanisms provided by Monitoring and Assessment Methods and Structured Risk Management. Together, these categories support a continuous cycle of risk awareness, mitigation, and improvement across the supply chain.

Throughout the guideline, emphasis is placed on the creation of essential documentation (e.g., supplier registers, incident response plans, contract templates) and the use of appropriate tooling (e.g., GRC systems, TPRM platforms) to ensure that the C-SCRM capability is both structured and sustainable.

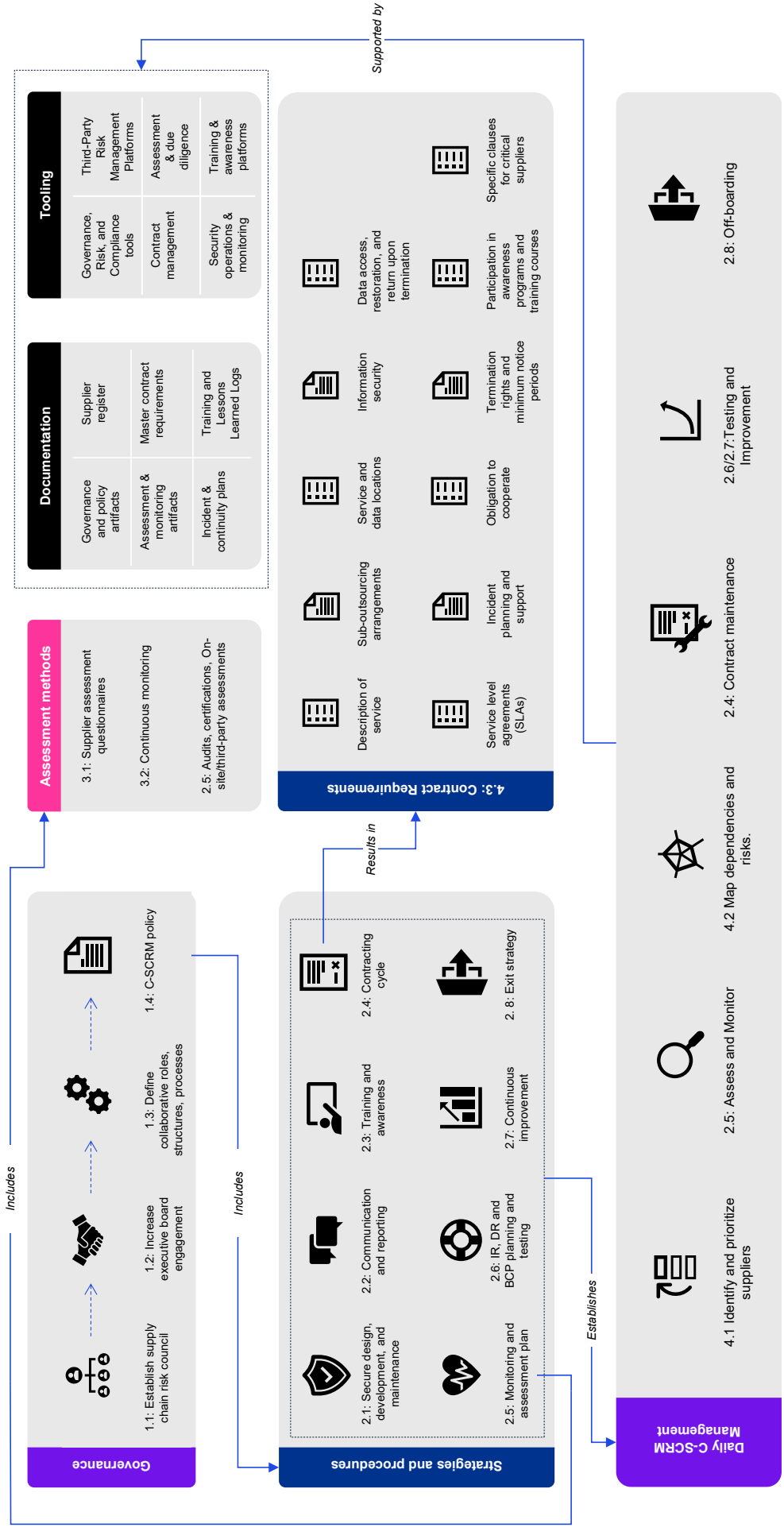


Figure 4.1: A visual representation of how our best practices implementation guideline is structured to establish a full C-SCRM capability within an organization.

4.1 Governance

Formally integrate supply chain risk considerations into the enterprise governance structure. This involves defining a C-SCRM strategy, policy, and implementation plan at the enterprise level, with leadership support and clear roles and responsibilities. The goal is to set the tone from the top and ensure organization-wide commitment to managing supply chain cybersecurity risks.

4.1.1 Establish a cross-functional supply chain risk council

Organizations need to establish a supply chain risk council that includes executives from across the organization (e.g., cyber, product security, procurement, legal, privacy, enterprise risk management, business units, etc.) This ensures a multidisciplinary approach to C-SCRM and supports collaboration and communication across departments.

- **Implementation**
  - Create a council of senior leaders with representation from the necessary and appropriate functional areas, including but not limited to: Cybersecurity/information security, Product security, Procurement/sourcing, Enterprise risk management (ERM), Legal, Business units (representing critical supply chain dependencies), Program management, Operations, IT,
  - Designate a program owner (e.g., CISO or a senior risk manager) who will be responsible for overseeing the implementation and ongoing management of C-SCRM practices.
  - Establish a formal charter that outlines the purpose, scope, membership, responsibilities, reporting structure, and meeting frequency of this council. The charter should clearly outline the council's authority and decision-making processes. Include measurable goals and performance metrics (e.g., percentage of critical suppliers assessed, number of incidents detected and mitigated) to track the program's progress and effectiveness.
  - Hold regular meetings to discuss key risks, develop mitigation strategies, monitor effectiveness, and report to senior leadership. The frequency of meetings should be determined based on the organization's risk profile and the urgency of issues. More guidance on council involvement can be found in best practice 4.1.2. Continuously monitor the effectiveness of the council's activities and make adjustments as needed.

    Ensure the C-SCRM program has the necessary resources (budget, personnel, technology) to effectively operate. This includes hiring or designating internal staff with relevant expertise in supply chain security and risk management. Provide funding for training, external consulting if required, and the tools necessary to assess and monitor supplier risks, such as risk assessment platforms, incident management systems, or third-party risk rating services. Determine ongoing resource requirements, such as the need for dedicated security staff to assess new suppliers or conduct regular supplier audits.
- **Objective**
  To establish a centralized, cross-functional council that brings together key stakeholders from across the organization to proactively review supply chain risks, set priorities, and direct the sharing of best practices. With this council in place, decisions can be made on the operation of an interdisciplinary approach at the mission, business process, and operational levels, effectively managing cybersecurity supply chain risks, aligning C-SCRM with business objectives, and ensuring resilience.
- **When to apply**
  This should be applied at the start of the C-SCRM implementation process. It is the foundational step that sets the stage for all other C-SCRM activities. Governance structures must be in place before any risk assessments or supplier evaluations can be effectively carried out, as they will provide the necessary authority, oversight, and resources to ensure the program's success. This recommendation is also ongoing as the program matures, it should be periodically revisited to adjust the governance framework as needed (e.g., as the organization grows or the threat landscape evolves). The complexity and formality of the council will scale with the size and complexity of the organization's supply chain. Smaller organizations might opt for a less formal structure, while larger, more complex organizations will benefit from a more structured approach.

- **Costs**
  Costs will vary depending on the size and complexity of the council. Primarily consists of personnel costs associated with council member participation. May also include costs associated with training and tooling.

  This includes the time and effort required to engage senior executives and secure their support may not involve direct costs but could be considered a hidden cost. Additionally costs associated with hiring or designating a C-SCRM program manager or team could incur costs. Additionally, there may be costs associated with investment in technologies or platforms for managing the C-SCRM function can add to the initial implementation costs.

  Ongoing costs will be endured for training both the C-SCRM team and other stakeholders involved in the process to ensure they remain up-to-date with best practices and emerging threats. This could involve both internal training costs or fees for external courses or certifications. As the program evolves, periodic adjustments may be necessary, such as upgrading tools, adjusting staff numbers, or increasing budget allocation for compliance.

- **Prerequisite conditions**
  Successful application hinges on committed and engaged executive leaders that together form a multidisciplinary front covering all aspects of the organizations departments. Clearly defined roles and responsibilities for each member are essential to avoid confusion and ensure accountability. The council must have the authority and resources to implement its recommendations. Open and transparent communication among council members and with other stakeholders is vital.

- **Cautions**
  The council should be efficient and avoid unnecessary bureaucracy, avoid creating a council that becomes a talking shop without real impact. The council should focus on the most critical risks and processes and avoid getting caught up in less significant issues that can be handled by working teams. The council's effectiveness should be regularly reviewed and the charter adjusted as needed.

4.1.2 Strengthen board oversight and engagement in C-SCRM

Successful integration of the C-SCRM program requires sufficient commitment, understanding and oversight from management. This requires procedures to ensure regular engagement with the executives.

- **Implementation**
  As established in best practice 4.1.1 the council charter should include reporting structures. This means that a formal policy must to be developed that establishes reporting arrangements, including the frequency, form, and content of reporting to the management body.

  Schedule regular presentations to the board (e.g., quarterly or annually) to provide updates on C-SCRM activities, key risks, mitigation strategies, and performance metrics. The frequency should be determined based on the organization's risk profile and the board's preferences.

  Create concise and informative presentations and reports tailored to the board's needs and understanding. Focus on high-level risks, key performance indicators (KPIs), and the overall effectiveness of the C-SCRM program.

  Encourage open dialogue and questions from the board members to ensure a thorough understanding of C-SCRM issues and challenges. This fosters a culture of transparency and accountability.

  Align C-SCRM reporting and discussions with the organization's overall enterprise risk management (ERM) framework. This ensures that C-SCRM is considered within the broader context of organizational risk.

- **Objective**
  To increase board-level understanding and oversight of C-SCRM, ensuring that the organization's C-SCRM strategy aligns with its overall business objectives and risk appetite. This elevates C-SCRM as a top business priority and ensures proper oversight.

- **When to apply**
  When establishing or maturing a C-SCRM program. Consider implementing early in the process to ensure organization-wide alignment. Larger organizations with more complex supply chains will likely benefit more from formal board-level engagement. Smaller organizations might opt for a less formal structure, while larger, more complex organizations will benefit from a more structured approach.

- **Costs**
  Costs will primarily involve staff time for preparing presentations and reports, as well as potential costs associated with training for board members

- **Prerequisite conditions**
  Strong support from senior management is crucial for securing board-level buy-in and resources. Develop clear and concise communication materials that effectively convey complex information to a non-technical audience. Use data and metrics to demonstrate the effectiveness of C-SCRM initiatives and justify resource allocation. Establish clear and measurable KPIs to track the progress and success of the C-SCRM program.

- **Cautions**
  Avoid overwhelming the board with technical details. Focus on strategic implications and key performance indicators. Keep presentations concise and focused on the most critical information. Adapt the language and level of detail to the board's understanding and expertise. Regularly review the effectiveness of board-level engagement and adjust the approach as needed.

4.1.3 Define and institutionalize collaborative roles, structures, and processes

Formal definition of roles, structures, and processes for C-SCRM in the organization facilitates efficient communication and collaboration throughout the entire organization while ensuring consistent implementation. This includes personnel involved in acquisition, management, execution, and monitoring of supply chain activities across internal functions (e.g., cybersecurity, supply chain, legal, physical security) and external entities (e.g., suppliers, developers, integrators, service providers).

- **Implementation**
  Define explicit roles at the enterprise, business, and operational levels to ensure accountability across the C-SCRM lifecycle. Include internal personnel (e.g., CISO, CIO, risk executive, program managers, engineers) and external stakeholders (e.g., suppliers' project/security managers), ensuring roles cover:
  - Risk identification, assessment, and mitigation
  - Contracting and acquisition
  - Security monitoring and incident response
  - Communication and coordination between stakeholders

  Create structures to facilitate collaboration, such as cross-functional teams, working groups, committees, or a C-SCRM project management office. These structures should have clearly defined membership, objectives, and reporting lines.

  The formality of this integration depends on the needs of the organization and can be structured as follows.
  - **Supply chain-led with security input:** The global sourcing team handles supply chain risk management, with information security teams providing cybersecurity-related inputs, including threats and security requirements. They conduct joint post-incident reviews and hold annual conferences to discuss developments in the threat landscape.
  - **Centralized team:** A centralized team manages risk across all supply categories, functioning like an internal audit team. They collaborate with information security, IT, legal, and compliance teams to perform risk assessments of all vendors. This approach simplifies supplier management and quickly addresses supply chain events or threats without escalating to executive leadership.
  - **Blended approach:** A centralized team provides guidance and oversight, while business units manage supplier relationships. The centralized team identifies risks, develops security requirements, approves supply chain changes, and operates as a service for the business. Business units select and manage their own suppliers, serving as principal managers for those relationships.

  When selecting an approach tailored to an organization it is paramount to take existing enterprise risk management processes into account. Integrate C-SCRM processess as much as possible into the existing frameworks, processes, and function. This ensures alignment with other organizational risk activities and prevents C-SCRM from becoming an isolated process. Develop standardized processes for communication, information sharing, and decision-making related to C-SCRM. This might include regular meetings, shared dashboards, and established escalation procedures. Herein, include both internal and external communication.

- **Objective**
  To promote transparency, accountability, and cohesive risk management practices across the supply chain by aligning internal and external stakeholders under clearly defined collaborative structures and responsibilities. This enhances communication, mitigates information asymmetry, and enables faster, coordinated responses to supply chain threats and vulnerabilities.

- **When to apply**
  During the development of a C-SCRM policy, at the initiation of new supplier relationships, and throughout the supplier lifecycle, including contract establishment and ongoing monitoring.

- **Costs**
  Costs will vary depending on the size and complexity of the organization and the chosen implementation approach. Primarily personnel costs associated with defining roles, establishing structures, providing training, and potentially hiring for new functions. Additional resources may be required to maintain collaboration tools and management oversight.
- **Prerequisite conditions**
  Clear understanding of existing roles and responsibilities within each function. Strong support from senior leadership is crucial for successful implementation. A culture of collaboration and information sharing is essential. Adequate resources (personnel, budget, tools) must be allocated to support the initiative. Effective communication and collaboration between the enterprise and its suppliers are essential for defining and agreeing upon roles and responsibilities. In addition, established processes and policies for managing supplier relationships and security are necessary to support the definition of roles and responsibilities and provide individuals with the needed mandates. Effective and secure communication channels and processes must be established.
- **Cautions**
  Avoid creating role confusion, conflicting roles, or duplication of effort. Ensure clear communication and reporting lines. The program should be flexible enough to adapt to changing circumstances and evolving threats.

4.1.4 Develop and maintain a comprehensive C-SCRM policy

C-SCRM procedures have to be formalized to ensure consistent execution throughout the organization and streamline communication and collaboration between departments. This is done by drafting an overarching C-SCRM policy. This policy must incorporate security requirements into every stage of a system and product lifecycle, from its initial design and development through deployment, operation, maintenance, and eventual decommissioning. Cybersecurity risks can and do materialize during all phases of the lifecycle and need to be adequately accounted for.

- **Implementation**
  When developing a C-SCRM function create formal documentation for procedures during their establishment. We establish a set of procedures that we bundle into an overarching C-SCRM policy. Drafting and continuously updating this policy and the included procedure as they are developed and implemented requires commitment, but minimizes ambiguity and ensures consistent and focused execution.

  The following procedures are necessary at minimum:

  - **Governance:** Record the establishment of the Supply chain council, its corresponding charter, and the roles, structures, and procedures, all detailed in best practice 4.1.1, 4.1.2, and 4.1.3 in the C-SCRM policy.
  - **Secure design, development, and maintenance:** All systems, applications, and services must be designed, developed, and maintained with security in mind following industry best practices for security. This includes ensuring secure coding practices, regular vulnerability assessments, and timely patching of security flaws. See best practice 4.2.1 for guidance.
  - **Communication and reporting:** Clear communication channels must be established between internal teams and third-party vendors regarding cybersecurity risks. Regular reporting of security incidents, vulnerabilities, and risk assessments should be conducted to ensure transparency. See best practice 4.2.2 for guidance.
  - **Training and awareness:** Regular cybersecurity training and awareness programs must be provided to all employees and third-party vendors to ensure that they are informed about the latest threats, organizational security policies, and best practices for securing systems and data. See best practice 4.2.3 for guidance.
  - **Contracting:** Any contractors engaged in providing services or products that interact with the organization's data or infrastructure must adhere to the same cybersecurity standards and practices outlined in this policy. The organization must ensure contractors are thoroughly vetted and evaluated for security risks. See best practice 4.2.4 for guidance.
  - **Monitoring and assessments:** suppliers must be subject to a combination of assessments and continuous monitoring to ensure security, compliance, and resilience. This includes vendor questionnaires, performance and risk monitoring, compliance audits, certification validation, and site visits, where appropriate. Assessment findings must be used to update supplier risk profiles and drive corrective actions. See best practice 4.2.5 for guidance.
  - **Incident response planning and testing:** Robust incident response, disaster recovery, and business continuity plans must be developed and regularly tested to ensure rapid recovery from any cybersecurity incident or disruption to operations. See best practice 4.2.6 for guidance.
  - **Continuous improvement:** The organization must continually assess and improve its cybersecurity practices and risk management strategies. Regular audits, assessments, and feedback loops should be established to ensure ongoing improvement. See best practice 4.2.7 for guidance.
  - **Exit strategy:** An exit strategy must be defined and implemented when terminating relationships with third-party vendors or subcontractors. This includes ensuring the secure transfer or destruction of data, deactivation of access credentials, and return of any proprietary assets. See best practice 4.2.8 for guidance.

  Align C-SCRM policy with enterprise risk management processes and policies so that supplier risks are considered alongside other risks. For example, include supply chain risk scenarios in enterprise

risk assessments and risk registers, utilize the same risk prioritization methods, and escalate supply chain risk decisions in line with corporate risk appetite thresholds.

Responsibility has to be assigned to a designated executive for overseeing the implementation and compliance with this policy. Regular audits will be conducted to ensure adherence to the guidelines outlined above. This policy must be reviewed and updated annually or when there are significant changes to the organization's cybersecurity landscape or regulatory requirements. These processes should be documented in the policy as well.

For each externally sourced service or product, the "need for" and the criticality of the procured service or product must be identified. Guidance on how to create such a procedure can be found in best practice 4.4.1.

A procedure on how to evaluate and select potential suppliers must be outlined. Guidance on how to create such a procedure can be found in best practice 4.2.5.

Define a list of standard requirements to adopt in contractual agreements with suppliers. This list should be used to guide the acquisition process and become explicit requirements for contract awarding. Guidance on how to create such a procedure can be found in best practice 4.4.3.

Create a cycle of reassessment intervals at which to review suppliers and their supplied products and services. Additionally, a set of off-cycle triggers has to be identified that would signal an alteration to the state of cybersecurity risks throughout the supply chain, such as policy, mission, change to the threat environment, enterprise architecture, SDLC, or requirements.

- **Objective**
  The primary objective is to proactively manage cybersecurity risks throughout the entire supply chain and the lifecycle of systems, products, and services. By defining a formal policy that integrates C-SCRM into each stage of the system and product lifecycle we create a standardized approach throughout the organization that enables efficient collaboration and communication between departments.
- **When to apply**
  Initial creation of the C-SCRM policy should be done when setting up or maturing a C-SCRM function. The level of detail and formality will depend on the criticality of the system or product and the organization's risk tolerance. Re-drafting and optimization of the policy should be done regularly to ensure alignment with business goals.
- **Costs**
  May include costs associated with training, tooling, and process changes. Costs will vary depending on the complexity of the system or product, the organization's existing security infrastructure, and the level of security expertise required.
- **Prerequisite conditions**
  The organization needs sufficient security expertise to guide the integration of security considerations throughout the life cycle or should acquire this expertise externally to ensure the right processes are created. Clearly defined processes and policies for implementing and monitoring C-SCRM throughout the life-cycle are necessary. Appropriate security tools and technologies are needed to support and streamline the implementation of security controls.
- **Cautions**
  Ensure that cybersecurity requirements are aligned with business objectives. avoid over engineering of systems and processes. Security should be integrated effectively without hindering functionality or usability Furthermore, maintaining comprehensive documentation and reporting on C-SCRM activities is essential for accountability and continuous improvement throughout the lifecycle.

4.2 Strategies and procedures

To effectively mitigate cyber supply chain risks, organizations must embed structured, adaptable strategies and procedures that reflect both internal priorities and external regulatory pressures. These strategies and procedures are then included in the overall C-SCRM policy as described in best practice 4.1.4. This section outlines best practices for developing actionable, repeatable strategies tailored to supply chain contexts. The recommendations aim to guide organizations in translating high-level policies into operational routines, ensuring coherence between enterprise-wide risk tolerance and day-to-day third-party engagements.

4.2.1 Embed security into system and product design, development, and maintenance

Incorporate cybersecurity controls and supply chain risk considerations into the design, development, deployment, and maintenance of products and systems. Doing so ensures that vulnerabilities are identified and mitigated early in the lifecycle, and that security remains a priority during updates and changes.

- **Implementation**
  Incorporate C-SCRM requirements into design and development specifications at initiation of the project.
  - To implement these requirements, **secure architecture practices** must be followed. This includes: Applying the principle of *least privilege* when designing access controls and data flows; Enforcing *network segmentation* to isolate critical system components; Using *secure-by-default* configurations for all services and system components; Ensuring *modularity and separation of duties* within the system architecture to limit the impact of a single compromised component.
  - During development, teams should adhere to **secure coding standards** relevant to their programming languages and platforms. These include practices such as: Avoiding the use of *deprecated or unsafe functions*; Implementing strict *input validation* and *output encoding*; Using *parameterized queries* to prevent injection attacks; Encrypting data at rest and in transit using strong *cryptographic protocols*.
  - Additionally, **security testing** must be embedded into the development workflow. This includes: *Static Application Security Testing (SAST)* during code check-ins; *Dynamic Application Security Testing (DAST)* during integration and system testing phases; *Dependency scanning* to identify known vulnerabilities in third-party libraries; Manual code reviews and threat modeling workshops, particularly for high-risk components.
  - Furthermore, a **hardened development environment** is needed. This includes: ensuring that *build and test environments mirror production configurations* as closely as possible; *Restricting developer access to production data*; *Enforcing version control* on all code repositories; *Logging* all administrative actions in development environments and conducting regular audits.
  - From a supply chain perspective, organizations should implement **supplier evaluation and validation procedures**. Every external component should be: Accompanied by a *Software Bill of Materials (SBOM)*; *Verified* through cryptographic signatures or checksums; *Monitored* for vulnerability disclosures throughout its lifecycle.
- **Objective** To proactively integrate cybersecurity considerations into the start of system and product life cycles, ensuring security becomes an integral part of the project and development pipelines.
- **When to apply** Initial creation of the procedure should be done when setting up or maturing a C-SCRM function. Then maintain throughout the entire lifecycle of systems, products, and services. It's not a one-time activity but a continuous process. Early integration during acquisition and SDLC phases is particularly critical. The level of detail and formality will depend on the criticality of the system or product and the organization's risk tolerance. Re-drafting and optimization of the procedure should be done regularly to ensure alignment with business goals.
- **Costs** Includes costs associated with training, tooling, and process changes. Costs will vary depending on the complexity of the systems and products, the size and maturity of the organization's

C-SCRM program, and the tools and technologies used.

- **Prerequisite conditions** Sufficient resources (personnel, budget, tools) must be allocated to support the implementation of security practices. Clear roles and responsibilities must be defined for all personnel involved in the design, development, and maintenance of systems and products. Appropriate security tools and technologies are needed to support and streamline the implementation of security controls.
- **Cautions** Ensure that cybersecurity requirements are aligned with business objectives. Avoid over engineering of systems and processes. Security should be integrated effectively without hindering functionality or usability Furthermore, maintaining comprehensive documentation and reporting on C-SCRM activities is essential for accountability and continuous improvement. Security practices should be reviewed and updated regularly to reflect changes in the threat landscape and best practices.

4.2.2 Implement robust C-SCRM communication and reporting mechanisms

Establish clear communication channels and reporting routines for supply chain cybersecurity risks. This ensures that relevant information flows to all stakeholders (operational teams, executives, regulatory entities, customers and suppliers) and that there is transparency and accountability in how supply chain risks are monitored and managed.

- **Implementation**
  - **Regular reporting:** Create a clear plan that outlines regular reporting cycles per stakeholder group and the information that should be reported.
    - **Enterprise level:** High-level summaries of overall supply chain risk posture, major incidents, and effectiveness of C-SCRM initiatives.
    - **Business process level:** Risk assessments specific to the mission/business process, status of mitigation efforts, and key supplier performance indicators.
    - **Operational level:** Detailed reports on vulnerabilities, incidents, and remediation efforts.
  - **Incident reporting:** Develop a clear incident reporting process, including escalation procedures for critical incidents and defined secure communication channels. In this process include plans for communicating with customers and regulatory entities in the event of a supply chain incident. Clearly define in which situations external certain external stakeholders are notified and which information should be provided herein.
  - **Roles, responsibilities, and channels:** Created designated roles and points of contacts for each identified stakeholder to create clear escalation plans and communication flows during specific situations. Define which communications channels can be used during these situations. Communicate these points of contacts and required communication channels to both internal and external contacts.
- **Objective** To establish clear communication channels and reporting procedures for managing risks effectively, ensuring transparency, accountability, and timely response to incidents through clear communication between organization departments, external stakeholders and suppliers.
- **When to apply** Initial creation of the procedure should be done when setting up or maturing a C-SCRM function. Re-drafting and optimization of the procedure should be done regularly to ensure alignment with business goals, regulatory requirements.
- **Costs** Largely involves internal time and software tools. There might be investment in a risk dashboard or tracking system to automate reports. Other costs are in staff time preparing and reviewing reports, and conducting meetings. These are generally moderate, routine costs of a risk management program.
- **Prerequisite conditions** Identification of stakeholders and an agreed-upon governance structure. Management should endorse open communication, inviting the disclosure of incidents and risks without retaliation.
- **Cautions** void information overload; ensure communication is concise and relevant. Maintain confidentiality where necessary. Regularly review and update the protocol to reflect changes in the threat landscape and best practices.

4.2.3 Implement role-based training and supply chain cybersecurity awareness

Implement a comprehensive training and awareness procedure focused on supply chain cybersecurity risks. The goal is to ensure that all relevant personnel including executives, technical staff, and procurement officers understand supply chain threats and know their role in managing these risks.

- **Implementation** Develop structured and role-specific training modules tailored to both internal stakeholders and external supplier personnel. The training should encompass the folowing.
  - **Role-specific training segmentation:** Segment the training according to roles within the organization. For instance:
    - **Procurement and vendor management teams:** Guidance on securely evaluating and contracting suppliers, establishing stringent supplier management policies, and recognizing signs of compromised procurement processes.
    - **Developers:** Instructions for securely integrating third-party components, recognizing malicious or tampered software updates, and maintaining secure coding practices as outlined in best practice 4.2.1.
    - **IT and security staff:** Methods for continuously monitoring supplier cybersecurity risks, identifying anomalous behaviors, and managing rapid response actions during cybersecurity incidents.
    - **Leadership:** Training focused on governance, oversight responsibilities, risk assessment, and the strategic integration of C-SCRM into organizational operations.
  - **Key topics:** Recommended subjects covered in training for internal stakeholders include:
    - Insider threat
    - Social engineering and mining
    - Suspicious communications and anomalous system behavior
    - Advanced persistent threat
    - Cyber threat environment
    - Physical security controls
    - Counterintelligence training
  - **Diverse training delivery methods:** Deliver training through various methods, including e-learning modules for foundational knowledge, workshops for interactive discussions, and periodic refresher communications (such as newsletters or intranet posts) to reinforce key points. Ensure that new hires whose roles involve supply chain interaction receive this training as part of their onboarding process.
  - **Incorporate practical exercises:** Where feasible, incorporate practical exercises. These may include scenario-based discussions, such as tabletop exercises simulating a supplier breach, or interactive simulations, such as phishing email tests appearing to come from supplier accounts, to ensure employees can apply their knowledge effectively.
  - **Regular training refreshers and updates:** Establish a schedule for regular refresher training, such as a mandatory annual training and update the content each cycle to address new threats, recent supply chain incidents, or changes in policy. Maintain records of completed training and follow up with individuals who are overdue.
  - **Continuous Awareness and Communication:** Continuously raise awareness through brief communications. For example, if a significant supply chain incident occurs, share a summary with relevant staff and highlight lessons learned. Similarly, share successes to reinforce positive behavior. For example, a team identifying and mitigating an issue before it becomes a problem.
  - **Supplier inclusion:** Determine which training and awareness activities should be attended by supplier personnel. Include clauses in contract agreements that establish these procedures

along with clauses requiring critical suppliers to maintain equivalent standards of cybersecurity awareness and training.

- **Objective** To cultivate an informed workforce capable of actively contributing to supply chain risk management. Training ensures personnel do not inadvertently introduce risks, such as selecting unvetted suppliers or mishandling supplier data, and that they can recognize and respond to supply chain security issues. This strengthens the overall security posture of the enterprise.
- **When to apply** Conduct formal training at least annually and during the onboarding of new relevant employees. Additionally, apply training whenever new processes or tools related to Cyber Supply Chain Risk Management (C-SCRM) are introduced, ensuring personnel understand how to use them securely. Implement ad-hoc refresher training in response to significant threats or incidents. Maintain an ongoing cadence of awareness throughout the year.
- **Costs** Costs associated with training include the development or purchase of training materials and the time employees spend in training instead of other work. Additional expenses may arise from training platforms or hiring external experts for specialized sessions. However, a well-trained staff can prevent incidents that would be far more costly, making the program a cost-effective investment in risk reduction.
- **Prerequisite conditions** Management support is essential to enforce training requirements and allocate the necessary time and budget. There must be an established understanding of key policies and procedures to translate into training content. Access to training delivery tools for e-learning or meeting platforms for workshops, is required. Identify target audience groups and their specific training needs in advance.
- **Cautions** Ensure the training remains relevant and engaging; stale or overly generic content may cause employees to disengage. Avoid one-size-fits-all modules that do not resonate with certain roles; instead, tailor content as needed. Be mindful of cultural and language differences when training a global workforce, ensuring that content is accessible and clear. Do not treat training as a checkbox activity; without periodic reinforcement and updates, even trained staff can become complacent or forget best practices.

4.2.4 Embed C-SCRM requirements into the supplier contracting lifecycle

Embed cybersecurity into the contracting cycle to ensure supplier risks are identified early, security obligations are formalized, and oversight is maintained throughout the relationship. This strengthens resilience, reduces disruptions, and supports regulatory compliance.

- **Implementation**
  - **Supplier classification:** To effectively manage cyber supply chain risk, organizations should establish a formal supplier classification process that categorizes suppliers into critical, important, and non-critical. This classification is based on factors such as the criticality of the goods or services being provided, the sensitivity of data involved, regulatory exposure, and the potential impact of cyber compromise. Once defined, these criteria should be applied consistently, and all suppliers should be recorded in a centralized supplier classification register. This register must be reviewed periodically to ensure it remains aligned with evolving risks, business needs, and regulatory expectations. Guidance on how to create this classification can be found in best practice 4.4.1.
  - **Pre-procurement assessment:** Before awarding contracts, suppliers should undergo a targeted security assessment. This involves issuing a standardized questionnaire aligned to industry frameworks such as ISO 27001, NIST, or SOC 2 report, and requiring documented evidence of the supplier's cybersecurity posture, including certifications, third-party audit reports, and details on risk governance practices. The responses should be evaluated against predefined scoring criteria to identify control gaps and inform contract negotiations. For suppliers delivering mission-critical services, the organization may also conduct independent security testing, on-site visits, or additional third-party assessments to validate controls and assess readiness. Guidance on supplier questionnaires can be found in best practice 4.3.1. General guidance on monitoring and assessmnets is provided through best praxctice 4.2.5.
  - **Master cybersecurity requirements:** A core part of embedding C-SCRM in contracts is developing a master cybersecurity requirements list, which defines the baseline security controls and obligations suppliers must meet. This list should cover a broad range of topics, including technical controls such as encryption, access management, data handling procedures, subcontractor management practices, and clear expectations around incident management and business continuity. The organization should map these requirements to each supplier criticality. To ensure consistency, these requirements should be embedded in all request for proposal templates, supplier selection criteria, and contract drafts. Guidance on creating master contract requirements is provided in best practice 4.4.3
  - **Contract negotiation and award:** The negotiation phase requires active collaboration between legal, procurement, cybersecurity, and relevant business units to ensure enforceable and balanced contract terms. Contracts should reference the organization's standard clause library, covering critical areas such as security obligations across the contract lifecycle, requirements for advance notification of material changes, and provisions for secure exit and transition. Throughout negotiations, any deviations or modifications to standard clauses should be tracked in a centralized contract management system, ensuring that the organization maintains visibility over supplier-specific risks and concessions made during the contracting process.
  - **Post-award monitoring and revalidation:** Once a contract is in place, organizations should leverage the embedded audit rights and monitoring provisions to maintain ongoing oversight of the supplier's cybersecurity posture. This includes requiring regular attestations, third-party certifications, or evidence of security control effectiveness, as well as monitoring supplier performance against agreed service levels. Suppliers should be reassessed and reclassified at least annually, or whenever material changes occur such as service expansions, mergers or acquisitions, major incidents, or regulatory developments. A robust post-award process ensures that supplier risk management does not stop at contract signing but remains active throughout the relationship. Guidance on this topic can be found in best practice 4.2.5.
  - **Contract exit and transition management:** Exit planning should be built into contracts, anticipating both the natural end of contracts and the possibility of early termination when serious problems arise. The contracting function must have clear authority to end agreements

if critical issues occur, such as repeated non-compliance, security breaches, or failure to meet key obligations. Contracts should define secure data return or destruction, transition assistance, and post-termination support, with clear timelines and responsibilities to minimize disruption. Organizations should also anticipate the end of supplier contracts in advance to allow for orderly transitions. After termination, a lessons-learned review should be conducted to strengthen future contracting and exit practices.

- **Objective** To integrate C-SCRM seamlessly across the entire contracting lifecycle, ensuring that security requirements are treated as qualifying criteria for supplier selection, incorporated into enforceable agreements, and continuously monitored throughout the relationship. This approach reduces the likelihood of supplier-induced disruptions, strengthens resilience, and ensures regulatory compliance.
- **When to apply** Initial creation of the procedure should be done when establishing or maturing a C-SCRM function. This procedure should be applied across all stages of the supplier engagement lifecycle, starting with request for proposal preparation, during supplier selection and contract negotiation, and continuing through post-award management. It is particularly important when engaging new suppliers, managing critical third parties, or renewing or terminating contracts. Review and adjust the approach regularly, especially when regulatory requirements, business priorities, or risk profiles change.
- **Costs** Costs primarily include staff time to develop and maintain master requirements, perform risk assessments, negotiate contracts, and perform post-award monitoring. There may be additional expenses for security assessments, third-party audits, or contract management tools. Although upfront and ongoing costs can be moderate to significant, they are offset by long-term savings from reduced incident response, regulatory penalties, and supply chain disruptions.
- **Prerequisite conditions** Successful implementation depends on documented internal security standards, and an established supplier risk classification process. Cross-functional alignment among procurement, legal, cybersecurity, and business stakeholders is critical. Access to contract management systems and risk assessment tools further supports effective execution.
- **Cautions** Avoid overloading smaller or lower-tier suppliers with excessive requirements that may strain their resources or impact delivery. Maintain flexibility in negotiations to balance enforceability with operational realities. Regularly update master requirements to reflect evolving threats, regulations, and lessons learned. Ensure that sensitive supplier assessment data is handled with strict confidentiality and shared only on a need-to-know basis within the organization.

4.2.5 Establish a comprehensive monitoring and assessment framework for suppliers

A robust C-SCRM program requires the use of multiple assessment and monitoring techniques to maintain ongoing visibility into the security, resilience, and compliance posture of external suppliers. Vendor questionnaires, continuous monitoring of third-party performance and risk, compliance audits, independent third-party assessments, site visits, and formal certifications provide complementary insights at different points in the supplier relationship lifecycle. By creating a strategy that establishes clear procedures on how to assess and monitor suppliers, organizations can identify emerging risks, verify compliance with contractual and regulatory requirements, and ensure that third parties supporting critical or important functions maintain adequate risk management practices throughout the engagement.

- **Implementation** Establish a formal multi-method assessment and monitoring program covering the entire supplier lifecycle. Techniques should include:
  - **Vendor questionnaires and self-assessments:** At supplier onboarding, and periodically thereafter, issue standardized questionnaires to critical and high-risk third parties. These questionnaires should gather detailed information about the supplier's cybersecurity controls, incident response processes, data protection practices, business continuity arrangements, regulatory compliance status, and any material changes since the previous review. Suppliers should be required to support their responses with evidence such as policies, certifications, or audit reports, rather than relying solely on self-attestation. Questionnaires should be updated over time to address emerging threats, regulatory changes, and lessons learned from past incidents. Responses must be systematically analyzed, and any red flags or deficiencies should feed directly into the supplier's overall risk rating and monitoring plan.
  - **Continuous monitoring:** Deploy continuous monitoring services and tools to provide real-time insights into third-party cybersecurity posture, operational performance, and risk indicators. Monitoring should encompass external attack surface evaluations, breach intelligence, regulatory enforcement actions, changes in corporate structure, financial health, and service performance metrics such as uptime and incident reporting frequency. Integrate monitoring outputs into supplier risk dashboards and internal risk reporting processes. Escalate significant negative changes in a supplier's risk profile to appropriate governance bodies, and initiate additional investigations or corrective measures as necessary. More guidance can be found in best practice 4.3.2
  - **Compliance audits:** Conduct formal audits of suppliers, particularly those supporting critical or regulated services, to validate compliance with contractual obligations, applicable laws and regulations, and industry best practices. Audits should examine evidence such as patch management logs, incident response records, vulnerability management programs, business continuity and disaster recovery test results, and compliance with agreed security standards like ISO/IEC 27001. Audit rights must be contractually established during procurement, and audit scope should be adjusted based on supplier criticality and evolving risk assessments as indicated in best practice 4.4.3. Findings must be formally reported, corrective action plans developed where necessary, and remediation progress tracked.
  - **Third-party assessments and certifications:** Rely on verified third-party certifications and independent assessment reports, where appropriate, as part of the assurance process. Acceptable certifications may include ISO/IEC 27001, SOC 2 report Type II, or industry-specific attestations, provided they are current and cover the relevant services, systems, and geographical operations. Certificates should be reviewed critically for scope and validity, and periodically refreshed. Where independent evidence is insufficient or not aligned to organizational risk tolerance, consider commissioning tailored security assessments to validate supplier controls directly.
  - **On-site assessments and visits:** Where appropriate, conduct physical site visits to suppliers supporting critical or sensitive functions. On-site assessments should evaluate physical security controls, secure handling and storage of sensitive data, staff compliance with cybersecurity policies, the robustness of backup and recovery arrangements, and readiness to detect and respond to security incidents. Site visits must be planned and documented, with findings feeding into the overall supplier risk evaluation. Visits should occur regularly based on sup-

plier criticality, typically on an annual or biannual basis, or whenever significant changes or incidents warrant additional scrutiny.

  - **Remediation acceptance criteria:** Define clear thresholds and acceptance criteria for remediation of identified security risks. These criteria should be tailored based on supplier criticality and the nature of the risk (CVSS scores, impact likelihood, non-compliance with contract terms). Establish timelines for remediation and require documented evidence of mitigation steps. Suppliers should not be removed from the "watch list" or considered compliant until revalidation confirms remediation effectiveness.
  - **Revalidation process:** After remediation is reported, initiate revalidation through reassessment, such as a follow-up audit, site visit, or review of evidence (e.g., patching logs, updated certifications). The revalidation process should be standardized and documented. In cases of high-risk findings, use independent third-party verification.
  - **Coordination and reporting:** All assessment and monitoring activities must be integrated into a centralized supplier risk management framework. Findings from questionnaires, monitoring tools, audits, third-party certifications, and site visits should be consolidated, analyzed holistically, and used to update supplier risk profiles. Significant risks and deficiencies must be reported to senior management and the risk governance committee, with recommendations for escalation, remediation, or contract renegotiation where necessary. Maintain a watchlist of suppliers who have had security issues in the past. This list indicates for which suppliers the organization should be more cautious and require additional due diligence, security requirements, and approval by the risk council. Continuous improvement loops must be established, ensuring that lessons learned from monitoring and assessments inform future supplier onboarding, contracting, and monitoring strategies.

- **Objective** To maintain a comprehensive and dynamic view of third-party risks over time, beyond initial due diligence. The aim is to ensure that suppliers remain aligned with security, resilience, and compliance expectations throughout the life of the contract. This enables early detection of emerging vulnerabilities, assurance of regulatory compliance, informed risk management decisions, and timely response to risks that could impact organizational operations, security, or reputation.
- **When to apply** The monitoring and assessment strategy should be created when establishing or maturing a C-SCRM function. This strategy should be applied throughout the entire third-party relationship lifecycle. Vendor questionnaires and initial assessments should be performed during onboarding and refreshed periodically. Continuous monitoring must operate during the entire engagement period. Compliance audits, site visits, and validation of third-party certifications should be conducted at regular intervals, based on risk tiering, or upon significant changes such as mergers, operational disruptions, security incidents, or regulatory developments. Assessments must also be triggered by incident response or new risk intelligence affecting a supplier.
- **Costs** Implementing a comprehensive assessment and monitoring framework entails both initial and ongoing costs. These may include personnel costs for performing assessments and monitoring activities, licensing fees for third-party risk monitoring tools, subscription fees for access to certification validation services, and costs associated with travel for on-site assessments. Organizations may also incur costs for engaging external auditors or consultants to conduct independent assessments. Strategic risk-based prioritization of suppliers can optimize resources and manage costs effectively.
- **Prerequisite conditions** Supplier contracts must clearly establish rights to audit, monitor, and assess, and suppliers must be obligated to cooperate. An accurate and current inventory of suppliers, categorized by criticality and risk exposure, must be maintained. Internal teams (procurement, information security, compliance, and risk management) must be trained in the assessment methodologies, and appropriate governance structures must be in place to oversee the monitoring program and respond to assessment findings.
- **Cautions** Organizations must guard against over-reliance on self-reported information in questionnaires without independent validation. Continuous monitoring services, while valuable, may not capture internal supplier risks hidden behind the external surface. Compliance audits and certifications must be reviewed critically to ensure they are meaningful and relevant to the services in scope. Overburdening suppliers with frequent or redundant assessments can strain relationships and co-

operation, especially with smaller vendors. Findings from assessments must not remain static or unaddressed. A defined process must exist for risk remediation, escalation, and ongoing improvement, ensuring that monitoring activities lead to actionable outcomes rather than administrative overhead. guidance for this can be found in best practice 4.2.7.

4.2.6 Develop and regularly test supplier-focused incident response plans

Establish and maintain a comprehensive Incident Response (IR), Disaster Recovery (DR), and Business Continuity Planning (BCP) capability that spans the organization and its critical suppliers. This involves defining roles, procedures, and resources to detect, contain, and recover from cyber or operational disruptions. The plan must cover both internal systems and key third-party dependencies, ensuring that incidents are promptly reported, evidence is preserved, and affected services are restored. In practice, this means creating coordinated processes for incident management: detection, triage, remediation, invoking backup operations when needed, and communicating with all stakeholders (internal teams, regulators, customers, supplier representatives) during a crisis.

- **Implementation**
  - **Establish an IR/DR/BCP team and policy:** Form a cross-functional response team (IT, security, operations, supply-chain representatives) and document authority levels and decision-making processes in case of an incident. Define an official policy or plan that describes how incidents are managed, how continuity plans are invoked, and who must be notified. Base these procedures on the classification of the incident in question, for example:
    * Low severity: Affects only a small number of systems or individuals, causes limited disruption to a few network devices or segments, or presents minimal or no risk of spreading and results in negligible disruption or damage.
    * Medium severity: Impacts a moderate number of systems and/or people, affects non-critical systems or services within the organization, or disrupts operations at a business unit level
    * High severity: Has a major negative effect on a large number of systems and/or personnel, creates significant financial or legal risks for the organization, compromises sensitive or confidential information, or impairs critical services or systems essential to core operations, or is highly likely to spread and result in severe disruptions or damage.

    Assign primary and alternate contacts for each critical function. Ensure the team includes members with expertise in both organizational processes and key supplier operations.
  - **Develop incident response, recovery, and continuity plans:** Draft detailed procedures for responding to disruptions. This includes steps to contain an incident, collect evidence for analysis, and invoke recovery plans when needed. For example, specify how to isolate affected systems, preserve logs, and escalate incidents to crisis management. Incorporate predefined thresholds or triggers (severity levels and impact criteria) that automatically activate the business continuity plan. Embed information security requirements into continuity processes, such as maintaining encryption and access controls even during failover.
  - **Include suppliers in plans and testing:** Integrate critical suppliers, as defined by best practice 4.4.1, into IR/DR planning and policy creation. Require that contracts obligate suppliers to immediately report relevant incidents and to assist in joint response exercises(best practice 4.4.3). Arrange regular testing activities (tabletop exercises or simulations) that involve both internal staff and representatives of critical suppliers. During these tests, simulate supply chain disruptions, e.g. a supplier outage, and practice supplier coordination. Jointly update procedures on lessons learned during these activities. Maintain an updated contact lists and communication protocols for each critical supplier so that all parties know when and how to coordinate during an incident.
  - **Maintain backup and failover resources:** Provision redundant infrastructure and reserves so critical operations can continue if primary assets fail. These backup assets ideally reside in a different geographical location. These assets combined should be able to ensure the organization can resume critical functions with minimal delay. Keep extra inventory or alternate supply channels for components that have no substitute. For example, it is recommended to hold 60–90 days of stock for the most critical hardware or arranging support agreements for priority replenishment. Document and periodically test data backups, hot-site failover procedures, and alternative work arrangements, such as remote work capabilities, to verify that recovery objectives will be met under various disaster scenarios.

- **Define communication and escalation procedures:** Specify exactly who should be informed during specific incidents and situations. This covers internal alerts and external notifications to regulators, customers, and critical suppliers. Use clear criteria to trigger alerts and crisis calls. Ensure that communications are timely but follow the "need-to-know" principle, with preapproved message templates to avoid confusion. After an incident, carry out a joint review, including affected suppliers, to perform root-cause analysis and update the plan based on lessons learned.
- **Regularly review and update the plans:** Schedule periodic reviews of the Incident Response (IR)/Disaster Recovery (DR)/Business Continuity Planning (BCP) documentation, at least annually or after any major organizational or environmental change. Update the plans to reflect new business processes, new suppliers, or emerging threats. Retest the plans after each significant revision. Conduct post-incident reviews even for minor events to identify gaps. Maintain logs of all tests and incidents to measure performance and drive continuous improvement.

- **Objective** Ensure the organization can absorb and recover from disruptions with minimal impact on critical business functions and supply chains. The IR/DR/BCP program aims to protect information confidentiality, integrity, and availability during crises, maintain agreed service levels, and meet legal or regulatory continuity requirements. By proactively planning and coordinating with suppliers, the organization minimizes downtime, avoids cascading failures, and preserves customer trust. A successful program prevents isolated incidents from becoming enterprise-wide outages, supports timely decision-making, and ensures that lessons learned are fed back into risk management.
- **When to apply** The monitoring and assessment strategy should be created when establishing or maturing a C-SCRM function. Tailor the implementation of this strategies to the needs of critical systems and services by creating specific IR, DR, and BCP plans before they go live. Reassess and reinforce it whenever significant changes occur, such as new regulatory mandates, major organizational restructuring, or onboarding of key vendors. Apply it after incidents to strengthen future response. Testing should occur at least annually and whenever environmental or supplier conditions change substantially.
- **Costs** Allocating staff time for policy development, plan writing, training, and exercises incurs significant internal costs. The establishment of a dedicated response team or committee may require the assignment or hiring of specialized personnel. Internal review and testing consume operational time. The ongoing maintenance of plans, including document updates and audits, contributes to recurring workload. Investments in backup sites or redundant infrastructure, such as alternate datacenters and cloud failover, along with additional inventory, entail capital or service fees. Organizations may incur higher contract rates or premiums to ensure supplier redundancy, including on-call backup production and priority logistics. Involving suppliers in drills may impose cost-sharing or fees for their participation. Technology investments in disaster recovery tools such as backup software and data replication, must be procured and maintained. Regular testing of continuity plans can temporarily disrupt normal schedules, such as taking systems offline or utilizing test data.
- **Prerequisite conditions** A clear risk management framework with strong executive support must be in place. Responsibility for overall crisis management should be well-defined. The organization should have completed a business impact analysis (BIA) or similar assessment to identify critical functions, assets, and dependencies, to determine which operations require the fastest recovery and what the consequences of downtime would be. Accurate inventories of IT assets, data, and suppliers are essential, along with a clear understanding of where critical data resides and which vendors support key processes. Supplier contracts should also be reviewed to confirm existing continuity requirements. It is paramount to ensure availability of alternate sites, backup hardware, and necessary personnel, in-house or through suppliers, to support recovery plan execution. This includes backup communication channels such as email failover or phone trees. Finally, contracts and policies should be reviewed to ensure they permit the necessary actions, such as audits and information sharing, and that they comply with regulatory obligations related to incident notification and continuity.
- **Cautions** Avoid focusing on only high-value contracts or obvious risks. Small suppliers providing

a niche component can be mission-critical. Planning should cover all critical processes and sub-tier dependencies. Continuity planning should be seen as an ongoing effort, not a one-time task, with plans that evolve alongside the business and its supply chain. Sensitive details, such as recovery site locations or encryption keys, should be shared only on need-to-know basis, since excessive disclosure can create additional security risks. Plans should strike a balance between rigor and flexibility. Overly complex or rigid procedures become unworkable in a real crisis, while allowing reasonable improvisation helps teams respond to unexpected situations. Relying solely on written procedures can cause problems as teams must be prepared to exercise judgment in critical situations. Regular testing is essential, plans that are never practiced often fail when needed. Organizations should avoid relying only on reactive approaches. Proactive measures, such as supplier monitoring and threat intelligence, should complement response planning.

4.2.7 Establish continuous improvement through feedback loops and reassessments

Continuous improvement embeds a feedback-driven cycle into the C-SCRM programto ensure that processes, controls, and policies are regularly refined. In practice, this means setting up formal mechanisms to collect performance data, review outcomes, and adjust C-SCRM measures over time. By institutionalizing lessons learned from incidents and supplier assessments, an organization can adapt its supply chain security posture to emerging threats and requirements.

- **Implementation**
  - **Define and collect metrics:** Identify internal key performance indicators (percentage of suppliers meeting a level of security requirements, time to remediate supply chain vulnerabilities, number of supply-related incidents) collected by the processes established through best practice 4.2.5. This data allows tracking C-SCRM performance against pre-determined goals.
  - **Establish governance review cycles:** Convene the cross-functional council established by best practice 4.1.1 at regular intervals as indicated by the procedure of best practice 4.1.2 to analyze the collected data. In these meetings, review supplier risk profiles, performance metrics, and any incidents. Use the insights to re-prioritize risks and adjust strategies.
  - **Embed feedback from incidents and assessments:** After any supply chain security incident, audit, or major supplier change, conduct a formal lessons-learned review. Document what worked or failed and update policies, standards, and controls accordingly. Ensure that remedial actions are tracked to completion as part of the improvement loop. share lessons learned both up and downstream to supply chain partners where applicable.
  - **Involve suppliers in joint learning:** Actively engage key suppliers in the review process. Establish protocols for bi-directional sharing of threat and risk information (vulnerability reports, threat intelligence) For example, organizations can hold joint tabletop exercises with critical suppliers to test response plans. Revise supplier contracts and service-level agreements to obligate suppliers to participate in these improvement activities based on the jointly aggregated data.
  - **Iterate and automate:** Use each review cycle's findings to refine C-SCRM processes. Update procedures established through best practice 4.1.4 based on feedback. Where practical, automate data collection and analysis through continuous monitoring tools and dashboards (best practice 4.2.5) to streamline reporting and free resources for analysis. Leverage frameworks, such as ISO/IEC 27001's Plan–Do–Check–Act approach or the NIST Cybersecurity Framework Implementation Tiers, to benchmark progress and guide maturity improvements.
- **Objective** To ensure the C-SCRM function remains effective and aligned with the organization's risk posture over time. It aims to create an adaptive, learning-based program in which every review and incident drives enhancements to security controls and risk management practices. By systematically integrating feedback, the C-SCRM program incrementally strengthens resilience and reduces risk. Continuous improvement ensures that supply chain security measures evolve as the observed threats and business context change.
- **When to apply** the continuous improvement procedure should be created when establishing or maturing the C-SCRM program. It is not a one-time task but a perpetual process throughout the supply chain and product lifecycle. Triggers for focused improvement reviews include major supply chain incidents or audit findings, significant changes in suppliers or technologies, regulatory updates, and scheduled intervals (annual management review).
- **Costs** Implementing a continuous improvement process involves investment in resources and tools. Organizations must allocate staff time and hire or train personnel, for data collection, metrics analysis, and committee meetings. Technology costs may include software for continuous monitoring, data analytics platforms, or third-party assessment services. There may also be costs for conducting supplier workshops or tabletop exercises. However, these investments can yield significant benefits: improved accountability, more efficient risk reduction, and cost avoidance from preventing or mitigating supply chain incidents.
- **Prerequisite conditions** For continuous improvement to be effective, the organization must first

have a basic C-SCRM infrastructure in place. This includes a defined governance structure, such as a risk council or program office, with clear accountability for metrics and actions. It also requires an up-to-date inventory of critical suppliers and assets, initial risk assessments, and formally documented policies. Established methods for collecting and analyzing supply chain security data, such as risk ratings, assessment results, and incident logs, are essential. Supplier agreements should include contractual clauses that allow for audits, sharing of security data, and require supplier cooperation in improvement activities. Equally important is strong executive leadership support, adequate budget for tools and training, and a culture that values iterative learning.

- **Cautions** It is important to avoid overloading staff and suppliers with too many metrics or frequent assessments. Prioritizing high-risk suppliers and core indicators helps prevent fatigue and ensures the data collected remains meaningful. Data gathering alone is not adequate enough. Findings must lead to concrete actions, as feedback loops without disciplined follow-up become box-checking exercises. Care should be taken to select relevant and reliable metrics, since using low quality or misleading indicators can create a false sense of security and may even encourage green washing during reporting. Oversight of suppliers should be balanced with collaboration, as excessive or redundant requests for information can damage supplier relationships. Joint forums or shared assessment frameworks can help manage this balance effectively. Finally, continuous improvement efforts must stay focused, avoiding scope creep. This ensures that the organization's efforts remain aligned with its risk tolerance and strategic goals, and improvements are both practical and relevant.

4.2.8 Plan for secure disengagement through defined exit and obsolescence strategies

Develop and maintain a formal exit strategy for all suppliers. This strategy ensures that if a relationship with a vendor must end, whether through planned contract expiration or unplanned failure, it can be executed with minimal disruption to operations. The exit strategy outlines how the organization will disengage from the provider, transition services or data, and maintain continuity of critical functions. By proactively preparing for termination scenarios, organizations avoid vendor lock-in, safeguard their data, and uphold resilience even if a key supplier is lost.

- **Implementation** Establish comprehensive procedures to plan, execute, and recover from the termination of third-party services. Key steps include:
  - **Plan from onboarding:** Integrate exit planning at the start of the vendor relationship. During procurement and contracting, evaluate the provider's proposed exit plan and negotiate explicit contract clauses for termination assistance, data handover, and continued service during transition. Define what constitutes the end-of-service in the agreement, such as criteria for contract completion, and ensure the contract mandates an adequate transition period with support commitments from the vendor for smooth handover. Create general master requirements that mandate this and include them in the master requirement list as described in best practice 4.4.3.
  - **Product obsolescence management:** Require suppliers to disclose EOL timelines, support sunset periods, and upgrade/replacement paths for critical products or components. Contracts should include clauses obligating suppliers to provide advance notice of planned obsolescence. Establish internal procedures for monitoring supplier product lifecycles. This includes identifying when alternative solutions or vendors will be needed and ensuring business continuity. Maintain a registry of critical product versions, their support status, and replacement strategy.
  - **Anticipate scenarios:** Identify trigger events and risks that might lead to termination. The strategy should address both planned exits (contract end-of-term, strategic provider replacement) and unplanned exits (provider insolvency, security breach, regulatory mandate, or other failures). For each scenario, document specific actions to take.
  - **Replacement strategy:** Outline how services can be migrated to an alternative solution when needed. This includes identifying one or more viable replacement providers or an internal capability that can assume the service. The plan must detail how to transfer operations and data to the new environment without compromising security or continuity.
  - **Data transfer and preservation:** Establish procedures for the secure return or transfer of all organizational data from the third-party. This involves scheduling data exports, verifying the completeness and integrity of returned data, and ensuring the third-party deletes or destroys any remaining sensitive data after the transition (per contractual obligation). Treat data custody as a priority: verify that backups are current and accessible in case the vendor abruptly ceases operations, and plan for how to quickly transfer those backups to the new environment.
  - **Continued operation during transition:** Plan for a defined transition period during which the outgoing provider continues to support services until the new solution is fully operational. Coordinate timelines so that there is overlap (when possible) to avoid gaps in service. During this phase, increase monitoring of performance and have staff on standby to address any incidents. If the exit is unplanned and immediate, invoke business continuity procedures (disaster recovery sites or pre-arranged interim services) to keep critical functions running. This should ensure that critical functions are never compromised during transitions.
  - **Roles and responsibilities:** create a cross-functional termination response team (IT, cybersecurity, procurement, legal, business continuity leads) responsible for executing the exit strategy. Clearly delineate who will manage communications with the vendor, who will handle technical migration tasks, who ensures contractual obligations are met, and who oversees continuity of operations internally. Establish an internal escalation process for approving and initiating an exit. Adopt training based on these plans in role based training programs as outlined in best practice 4.2.3.

  - **Testing and updates:** Regularly test and review the exit strategy. This can involve tabletop exercises or simulations of provider loss to ensure staff are familiar with the procedures and to uncover any weaknesses in the plan. For critical providers, consider conducting joint drills or discussions with the vendor about how a transition would work. Update the strategy whenever there are significant changes (changes in regulation, corporate structure, services, demands, strategy). Ensuring the exit strategy remains sufficiently tested and reviewed periodically.
  - **Execution and recovery:** When termination is enacted, follow the established checklist to execute the exit in a controlled manner. Maintain detailed logs of all actions (communications, data transfers, system cut-offs, access revocations) for audit and accountability. Throughout execution, communicate status to all relevant parties (internal management, outgoing vendor, incoming vendor, regulators, and clients if service might be impacted). After disengagement, verify that the new provider or internal system is functioning correctly and that all security controls are in place. Conduct a post-termination review to capture lessons learned and incorporate improvements into the strategy. Also confirm the old vendor has fulfilled all end-of-contract duties (such as confirmation of data deletion and return of equipment or credentials).

- **Objective** The primary goal of the exit strategy is to ensure the organization can seamlessly disengage from a third-party provider without jeopardizing operations or security. It is a safeguard for business continuity and operational resilience during vendor transitions. By having a well-defined and practiced exit plan, the organization protects itself from service disruptions, data loss, compliance violations, or financial and reputational damage that could occur if a key supplier's services are suddenly unavailable. In essence, this strategy preserves the integrity and availability of critical functions under all circumstances by anticipating and mitigating the risks of a supplier relationship ending. It strengthens the organization's negotiating position with providers and ensures compliance with industry regulations that mandate continuity planning for outsourced services.
- **When to apply** Create a general exit strategy when establishing or maturing the C-SCRM function. Modify and apply this exit strategy for every third-party service that supports critical or important business functions at the outset of the engagement. This should be a standard part of onboarding any high-impact vendor. The exit strategy should be formulated during vendor selection and pre-contract risk assessment, and the agreed plan should be documented in the contract. Thereafter, review and update the exit plan at least annually or whenever there is a significant change in either the provider's or the organization's circumstances (changes in regulation, corporate structure, services, demands, strategy). Activation of the exit strategy should occur whenever predetermined conditions or triggers are met. These triggers can include strategic decisions, performance issues, financial or operational or legal issues on the vendor's side. For suppliers that are not deemed critical, it is possible to fall back on the general exit strategy and scale it to the inherent risk or the supplier.
- **Costs** Initial costs may include the effort required to develop detailed exit procedures and the possible investment in backup solutions or dual sourcing. Negotiating robust exit clauses might slightly increase legal or procurement expenses, and some vendors may incorporate the added responsibilities into their pricing structures. In addition, there are ongoing costs associated with periodically testing the exit process, which will consume staff time and incur fees if suppliers are involved. Regular governance efforts are also necessary to keep documentation and contracts updated. Maintaining the ability to exit may necessitate paying for data portability features or additional data export tools from the provider. A well-executed exit strategy can prevent costly downtime, avoid regulatory fines, and minimize the need for emergency IT projects to replace a lost service. Incorporating exit provisions early in the contract can result in cost savings by clarifying responsibilities, avoiding litigation, or consulting fees during termination.
- **Prerequisite conditions** The organization should have a clear understanding of its third-party dependencies through an up-to-date inventory or register of all ICT services and their associated providers. Identifying which vendors support critical functions is a prerequisite to prioritize where detailed exit plans are needed. There must be strong governance and support for C-SCRM from executive leadership that endorses the importance of exit strategies. Additionally, the organization should have its business continuity and disaster recovery capabilities aligned with the exit strategy.

- **Cautions** Avoid complacency, an exit plan can become obsolete if not kept up to date. Regular reviews are essential to ensure the plan reflects current systems, data volumes, and business requirements. otherwise, a well-intended plan might fail when needed. Build in some adaptability and clear decision points so that those executing the plan can respond to the specifics of the situation. During execution, manage communications with the provider carefully to maintain their cooperation. Maintain strict security measures throughout the transition.

4.3 Monitoring and assessment methods

Ongoing oversight and assessment are crucial components of a mature C-SCRM framework. Without robust mechanisms to continuously monitor and evaluate third-party risk exposure, even the most carefully constructed strategies may become ineffective over time. This section introduces best practices for establishing transparent, scalable, and efficient monitoring and assessment processes, with a focus on leveraging both automated tools and human oversight to detect, evaluate, and respond to emerging threats across the supply chain lifecycle.

4.3.1 Leverage standardized security due diligence tools to assess supplier risk profiles

A Supplier Risk Questionnaire Assessment is a structured survey sent to suppliers to gather detailed information about their cybersecurity, privacy, resilience, and compliance practices. This standardized questionnaire uses predefined questions and scoring rules so that supplier responses can be objectively evaluated. Responses are scored against risk factors to produce a total risk rating. By normalizing the questions and scoring, organizations obtain consistent, comparable risk data across all suppliers.

- **Implementation**
  - **Design the questionnaire content:** Define key risk categories such as information security, data privacy, business continuity, regulatory compliance, and map questions to relevant standards or controls adopted in acquiring organization. Use clear and unambiguous questions with standardized response options (Yes/No or 1–5 scales). Follow a point-based method: each question or answer is assigned a numeric value, and critical questions may carry higher weight. Sector organizations may have created generalized templates to adopt in specific industries, adopt these where possible. Ensure the questionnaire is applicable to all supplier types by adjusting language or sections for product suppliers, service providers, etc.
  - **Select distribution tools and workflow:** Use a secure survey or vendor-management platform to distribute the questionnaire. Many organizations integrate this into their procurement or GRC/ERP systems so suppliers can log in and complete assessments online. The tool should ideally auto-calculate scores based on predefined criteria. Establish an automated workflow: for instance, once a supplier contact is identified, a system can email the supplier a link or template and later send reminders if there is no response. Link the completed questionnaire to the procurement record to maintain an audit trail.
  - **Scoring and analysis:** Define a scoring methodology up front. For each response, assign points according to the risk level (e.g. critical=1/high risk, up to 5=low risk). Allow subject-matter experts (SMEs) in IT, legal, compliance, etc. to score sections relevant to their domain. Sum the points (with weightings applied) to compute each supplier's total risk score. Once scores are calculated, lock them in (scores should remain static throughout the review to ensure objectivity). Classify suppliers (e.g. high/medium/low risk) based on thresholds or risk categories derived from these scores.
  - **Review and follow-up:** Examine the questionnaire results. Discuss any significant findings or inconsistencies. For high-risk scores or gaps in critical controls, engage directly with the supplier to clarify answers or require remediation. Document all discussions and decisions. Update the enterprise risk register or third-party risk platform with the assessment results and any action items. Incorporate this data into ongoing supplier monitoring and risk treatment plans.
  - **Frequency and updates:** Issue questionnaires at the start of procurement processes to be able to quantitatively compare potential suppliers and require a certain level of security for contract awarding. Establish clauses in the contractual agreement on time-frames and procedures for mitigation of any found risks or vulnerabilities. After contract establishment issue questionnaires on a scheduled basis (for example, annually or upon contract renewal) to catch changes in supplier risk over time. Also trigger reassessments after major events (supplier mergers/acquisitions, geopolitical changes, significant incidents, or new regulations). This initial assessment is a snapshot in time, and continuous monitoring is needed throughout the

supplier lifecycle as established by best-practice 4.3.2. Regular updates to the questionnaire are necessary to reflect new threats, technologies, or regulatory requirements.

–

- **Objective** To systematically gather supplier risk data and support objective decision-making. The questionnaire ensures all suppliers are evaluated against the same criteria, making comparisons and prioritization reliable. This consistent approach feeds into the organization's overall risk management strategy and provides documented evidence of due diligence, helping to satisfy regulatory requirements.
- **When to apply**
  - **Initial onboarding:** Deploy to all new suppliers as part of due diligence, before contracts are finalized.
  - **Periodic reviews:** Conduct at regular intervals (e.g., annually, biannually) or at each major contract renewal. Higher-risk suppliers (critical to operations or handling sensitive data) should be reassessed more frequently.
  - **Event-driven:** Reissue the questionnaire after significant changes (major product or service updates, leadership changes, security incidents affecting the supplier, etc.) or when new compliance mandates arise.
  - **All supplier types:** Apply to vendors of products, services, and cloud/IT resources. Customize sections as needed (e.g., supply chain integrity for component manufacturers, data handling for cloud providers). By covering the full supplier base, organizations maintain visibility into any potential weak links in the supply chain.
- **Costs** Initial costs include time to design the questionnaire, configure tools or systems, and train staff. Many organizations reduce effort by leveraging existing templates. There may be licensing or subscription costs for survey/GRC platforms, but these often pay off by automating manual tasks. Ongoing costs involve analyst time to review responses and follow up. However, using workflow automation and risk tools can significantly cut labor costs and errors; for example, systems that auto-route questionnaires and scoring greatly reduce the need for manual process and improve efficiency.
- **Prerequisite conditions** To implement supplier risk questionnaires effectively, organizations must have a defined governance structure or formal C-SCRM policy that outlines assessment criteria and responsibilities. A current supplier inventory, categorized by criticality or risk level, is essential for targeting questionnaires appropriately. A baseline risk framework must also be in place to evaluate responses meaningfully. Tools such as secure survey platforms or third-party risk systems should support distribution and analysis; where not available, manual processes must ensure data confidentiality and integrity. Success further depends on coordinated involvement from procurement, cybersecurity, legal, and compliance teams, all of whom must agree on the process scope and timeline.
- **Cautions** Excessive or overlapping questionnaires can cause supplier fatigue, resulting in lower-quality responses. Internal coordination and the use of standardized or shared assessments can help reduce this burden. Self-reported data may also be biased or incomplete, so critical risks should be validated through audits or direct engagement. Since assessments are point-in-time, they should be complemented by continuous monitoring of emerging risks. Additionally, automation tools may have limitations and must safeguard sensitive supplier data. Finally, organizations should keep questionnaires focused and legally supported to encourage transparency and supplier cooperation.

4.3.2 Implement continuous monitoring across enterprise and supply chain

Establish and maintain a continuous monitoring strategy to proactively oversee cybersecurity risks across both internal enterprise systems and the extended supply chain. This strategy entails the ongoing surveillance of organizational assets, networks, and applications, as well as the continuous evaluation of security postures and service performance of suppliers. The goal is to detect changes in risk conditions or compliance status in real time and address issues before they escalate. Because one-time risk assessments provide only a snapshot in time and can become obsolete as environments evolve, a continuous monitoring approach ensures that emerging threats, vulnerabilities, or deviations are adequately identified and mitigated.

- **Implementation** Develop and integrate a comprehensive continuous monitoring plan that covers key assets, processes, and suppliers.
  - **Internal continuous monitoring:** Continuously monitor the enterprise's own networks, systems, and data for signs of anomalous activity, vulnerabilities, or policy non-compliance. Deploy technical controls such as automated vulnerability scanning, intrusion detection systems (IDS/IPS), security information and event management (SIEM) tools, and configuration monitoring to collect real-time telemetry. Define appropriate indicators and alert thresholds for suspicious behavior (unusual network usage patterns, after-hours access, unrecognized devices). Ensure that monitoring processes encompass all critical IT assets and business processes, including cloud services and operational technology, to enable prompt detection of intrusions or failures. Integrate supply chain considerations into these processes, for example, correlate logs related to third-party connections or data exchanges, so that supplier-related anomalies can be quickly recognized as such. All monitoring data should feed into a centralized analysis function such as a Security Operations Center (SOC) for continuous review and correlation.
  - **External Continuous Supplier Monitoring:** Extend the monitoring strategy to cover third-party service providers, suppliers, and contractors, especially those supporting critical or important functions. The organization's supplier risk management team (or equivalent function) should actively and regularly assess supplier security posture and performance throughout the life cycle of the engagement. Determine in which capacity this is necesarry for your organization. From scanning public domains of suppliers to assess their security level, to monitoring the full internal landscape, and everything in between. Implement processes to collect supplier performance data through automated feeds, third-party services, such as cybersecurity ratings or threat intelligence services, and direct supplier reporting. Metrics to monitor should include:
    - **Operational performance indicators:** uptime, support response times, SLA adherence
    - **Security metrics:** data confidentiality breaches, unauthorized access incidents
    - **Compliance measures:** certification status, regulatory adherence
  - **Security metrics to monitor:** The following security metrics should be continuously monitored where possible to maintain a clear and up-to-date understanding of the organization's cybersecurity posture and the state of risks within its extended supply chain. Tracking these parameters enables early detection and timely response to emerging threats or vulnerabilities:
    - **Software patching:** Status of software patches for application servers, OpenSSL, CMS, and web servers, including identification of end-of-life or vulnerable software.
    - **Application security:** Assessment of adherence to security practices such as CMS authentication, HTTP security headers, encryption for high-value systems, and malicious code detection.
    - **Web encryption:** Configuration data regarding web encryption, including certificate validity and expiration, hash algorithms, key lengths, encryption protocols, and certificate subjects.
    - **Network filtering:** Data on exposure of unsafe network services and IoT device vulnerabilities.

    - **Breach events:** Records summarizing organizational breach incidents, indicating frequency and severity.
    - **Malicious infrastructure connections:** Monitoring data of communications with command and control servers, botnet hosts, hostile scanning or hacking hosts, phishing sites, spamming hosts, and other blacklisted entities.
    - **Email security:** Email service configurations, tracking encryption standards (STARTTLS), and authentication mechanisms (SPF, DKIM), along with email hosting provider details.
    - **DNS security:** Status of protections against unauthorized DNS modifications and domain hijacking, including DNS hosting arrangements.
    - **System hosting:** Analysis of hosting environments, specifically co-tenant IP hosting scenarios, hosting fragmentation, and geographical distribution of hosting providers.

  This can be done through several technical services provided by third parties to implement this as a cost-efficient solution.

- **Objective** To maintain an up-to-date understanding of both internal and supply chain risks and to enable proactive risk mitigation. Continuous monitoring ensures that emerging threats, supplier performance issues, or compliance lapses are discovered early, allowing the organization to respond before they impact operations. The objective is to continuously verify that both the organization and its critical suppliers adhere to required security standards and to promptly address any weakness or change that could increase risks, preserving operational resilience and trust in the supply chain. The aggregated data and indicators can be used to shape improvement initiatives to evolve the C-SCRM function throughout.
- **When to apply** This strategy is applied on an ongoing basis throughout the operational lifecycle of systems and supplier relationships. Continuous monitoring should be established once initial risk controls are in place and continue as long as the asset or supplier remains in use. Monitoring activities run continuously or at defined frequent intervals depending on organizational needs. Combine real-time alerts with monthly or quarterly risk reviews.
- **Costs** This strategy involves investment in both technology and personnel. Tooling and technology costs can include security monitoring systems, such as SIEM platforms for log and alert management, vulnerability management tools, and subscriptions to threat intelligence or third-party risk monitoring services. For supplier monitoring, additional tools or services may be used to gather and analyze supplier cybersecurity ratings, news feeds, or compliance reports. Personnel costs are related to skilled staff or service providers needed to set up and maintain monitoring tools, analyze alerts, perform supplier audits, and manage the flow of information. Organizations may engage external vendors for continuous supplier risk intelligence, which incurs subscription or consulting fees.
- **Prerequisite conditions** Organizations need a baseline understanding of its assets and supply chain: an up-to-date inventory of critical information systems, components, and suppliers, along with an initial risk assessment for each, provides the foundation on which to monitor changes. A defined C-SCRM policy and risk appetite must exist so that monitoring efforts know what thresholds of risk are acceptable and what triggers should prompt action. Internally, the technical infrastructure for monitoring should be established: logging and event management systems configured on key assets, network monitoring, and vulnerability scanning processes. For external parties, the organization should ensure that contractual agreements with critical suppliers include provisions enabling continuous oversight. This entails having clauses that require suppliers to provide security transparency as stated in best practice 4.4.3. Assign clear roles and responsibilities for monitoring activities: teams or individuals must be empowered and trained to carry out continuous monitoring. Defined procedures are needed for what to do when a warning or anomaly is detected (best practice 4.2.6). Organizations should establish secure channels and processes for information sharing with suppliers, agreeing on how threat intelligence or incident reports will be exchanged, to facilitate the smooth flow of information needed for monitoring.
- **Cautions** Alert fatigue arises when monitoring systems generate too many alerts, especially false positives, causing staff to become overwhelmed and risk missing real issues. To prevent this, alert

thresholds must be carefully tuned, and trained personnel should review alerts promptly. While automation and external risk ratings are valuable, they should be complemented with human judgment, manual reviews, and supplier engagement, as automated tools can miss important context. Acting on identified issues is critical, without follow-up, monitoring creates a false sense of security. Organizations need clear processes to prioritize and fix both internal and supplier-related risks, keeping leadership informed to support necessary actions. Data collection alone is not enough; the focus must be on meaningful analysis and follow-through. Additionally, excessive or repetitive assessments can strain supplier relationships, so companies should focus on critical metrics and use coordinated or shared assessments where possible.

4.4 Structured risk management

Cyber supply chain risk must be managed proactively through a structured, lifecycle-based approach that integrates identification, analysis, treatment, and communication of risk. This section provides guidance on designing a comprehensive risk management process. The aim is to equip organizations with a coherent methodology for prioritizing risk scenarios, assigning responsibilities, and integrating feedback loops that foster continuous improvement and resilience in supplier relationships.

4.4.1 Identify, inventorize, and prioritize supply chain components

Develop a comprehensive inventory of the organization's ICT supply chain components including hardware, software, cloud services, and vendors and determine which of these are most critical to your business operations. By identifying "crown jewel" systems/data and their dependent suppliers, you can focus risk management efforts where a supplier failure or compromise would have the greatest impact. This step establishes a clear view of who and what you rely on, and which dependencies warrant the highest scrutiny.

- **Implementation** Identifying critical suppliers can be done either bottom-up or top-down. Depending on the organization's needs or already established inventories.
  - **Inventorize:** The top-down approach begins by identifying business processes or functions that are crucial to the organization's mission or required for legal compliance. This creates an inventory of functions that, if disrupted, could cause major operational, financial, or reputational harm. From this inventory supplier identification can be prioritized based on the most critical functions This approach is recommended when there is a mature enterprise risk management function that can provide an existing inventory.

    For each item in the inventory, starting with the most critical functions, document which external ICT products and services the organization support this function. This includes suppliers of hardware devices, software applications, open-source components, cloud and SaaS providers, managed service providers, data providers, etc. Catalog key details for each, such as the supplier name, what product/service they provide, and which internal system or business process it supports.

    The bottom-up approach begins by creating or updating an inventory of all external ICT products and services the organization uses. This includes suppliers of hardware devices, software applications, open-source components, cloud and SaaS providers, managed service providers, data providers, etc. This approach is recommended when there is a mature IT function that can provide an existing inventory. For each item in the inventory, document which business function or process relies on it. Identify where suppliers support functions that are essential to your organization's mission or legally required services.
  - **Prioritize:** Establish criteria to evaluate how critical a supplier or supplied component is. Possible methods are:
    - **Business impact:** Suppliers are rated based on the potential consequences their failure or compromise could have on the organization. This includes assessing their role in product delivery, the availability of alternative sources, and the cybersecurity risks they pose. Suppliers with access to the organization's network or facilities are deemed more critical and are often subject to continuous security monitoring.
    - **Stability:** The long-term viability of a supplier is crucial. If a supplier shows signs of instability, organizations may need to find alternatives, modify the product, internalize production, or discontinue the product's supply.
    - **Delivery impact:** The effect of supply disruptions and the cost of securing alternative sources are considered. Strong relationships with suppliers help organizations understand their operations and risk profiles, which in turn determines their criticality.
    - **Additional criteria:**
      - Suppliers with access to sensitive information, intellectual property, or regulated data, are classified as highly critical.

· Suppliers contributing to long-term strategic initiatives are given greater importance.

· The potential impact on the consistency and availability of the organization's products also influences a supplier's criticality.

Classify suppliers/products as critical, important, and non-critical based on these factors. Document why each obtains their specific criticality classification (this will inform tailored controls in later stages). Compile this list of classifications in a manageable register.

– **Validation:** Review the critical supplier list with business owners and IT owners to ensure no critical dependency is missed. Often, department heads know which vendors are mission-critical. This collaboration also builds awareness that those suppliers need stronger risk management.

– **Maintain:** Implement a process to keep the supplier and asset inventory up to date, such as when onboarding new suppliers or when systems are retired. Leverage automation if possible to track components. (In advanced scenarios it is possible to use centralized asset repositories with supply chain metadata, and even automated tools to detect new components.

- **Objective** To gain visibility into the supply chain and pinpoint where a cyber incident at a supplier could significantly disrupt the organization. By knowing which suppliers and components are most critical, the organization can allocate C-SCRM resources efficiently and apply stricter controls or monitoring to those areas. This ensures that later steps are risk-driven by identifying those critical dependencies upfront.
- **When to apply** Conduct this identification as one of the initial activities after establishing governance. It should be performed early, prior to engaging in risk assessments or controls, as it determines scope and priorities. Update the critical supplier list periodically (annually) or whenever significant changes occur, such as the introduction of a major new supplier or business changes. Additionally, revisit the list in response to major external events, such as the emergence of a new systemic vulnerability that may elevate the criticality of a particular software supplier overnight.
- **Costs** This step primarily involves staff time for information gathering and analysis. Tools such as spreadsheets or existing asset management databases can be utilized; specialized vendor inventory tools are optional. The most significant cost may be the time spent by various departments to enumerate and review their suppliers. However, this foundational work often overlaps with existing IT asset management or business continuity planning efforts, minimizing additional costs.
- **Prerequisite conditions** A basic understanding of the organization's business processes and existing IT asset inventory. If the organization has conducted a Business Impact Analysis (BIA) or similar, this can provide valuable input for identifying critical functions and supporting suppliers. Ensure access to procurement records or accounts payable data to enumerate suppliers if an official inventory is not in place.
- **Cautions** Avoid solely focusing on the monetary value of contracts, a low-cost software library could be more critical (security-wise) than an expensive office supplies contract. Do not treat this as a one-time checklist; if not maintained, the inventory will become outdated as the supply chain evolves. Lastly, respect confidentiality when gathering supplier information and avoid broadly exposing sensitive supplier details within the company.

4.4.2 Map supply chain dependencies and sub-tier risks

Go beyond immediate (tier-1) suppliers and develop an understanding of the broader supply chain for critical products and services. This involves identifying the key sub-suppliers, geographies, and other dependencies that lie upstream of direct suppliers. By mapping out these relationships and dependencies, the organization can anticipate and mitigate risks arising from deeper in the supply chain (such as concentration risk, geopolitical issues, or single points of failure hidden at lower tiers). This step consists of achieving visibility and insight into the complete supply chain.

- **Implementation**
  - **Link critical functions to suppliers:** Use the inventory of critical assets and processes (see best practice 4.4.1) to identify which external products, services, and providers are critical or essential. Map these dependencies explicitly, including hardware, software, cloud services, and third-party support.
  - **Map upstream and sub-tier dependencies:** For each critical supplier, systematically identify key sub-suppliers, outsourced service providers, and geographic locations tied to production or delivery. Use supplier questionnaires, audits, or open-source intelligence to obtain this data. Request transparency on critical components, such as whether software relies on specific third-party libraries or whether hardware depends on manufacturing concentrated in high-risk regions.

    Leverage technical tools: Use tools such as Software Bills of Materials (SBOMs) to uncover third-party libraries, firmware elements, and open-source components in software products. Maintain inventories of hardware components and sourcing locations. Supply chain management platforms or visualization tools can help link this information into a comprehensive, multi-tier dependency map.
  - **Classify and prioritize risks:** Evaluate risks based on criteria such as geographic clustering (e.g. concentration of suppliers in a single region), lack of redundancy, dependency on niche providers, or exposure to geopolitical instability. This prioritization helps focus mapping and mitigation on the most consequential dependencies.
  - **Maintain and integrate the map:** Build a structured, living supply chain map (such as a layered diagram or digital register) that captures both direct and sub-tier relationships. Integrate this map into enterprise risk management, continuity planning, and supplier onboarding or reassessment processes. Ensure it is accessible to relevant internal stakeholders.
  - **Review and update:** Revalidate the dependency map during supplier requalification, contract renewal, or when significant changes occur in products, services, or global conditions. Incorporate insights from disruptions, supply chain incidents, or threat intelligence to refine the map and improve the understanding of upstream risk.
- **Objective** To achieve end-to-end visibility into supply chain relationships, enabling proactive identification of single points of failure, hidden interdependencies, and high-risk pathways. This supports effective incident response, business continuity, and compliance with regulatory requirements.
- **When to apply** Perform initial mapping when establishing the C-SCRM program, when introducing new critical suppliers, or when significant business or technology changes occur. Update regularly (e.g., annually or during major contract renewals) to reflect evolving supply chain structures.
- **Costs** Primarily staff time for data collection, supplier engagement, and maintenance, as well as potential expenses for mapping software or Software Bills of Materials (SBOMs) tools.
- **Prerequisite conditions** An accurate inventory of critical assets and primary suppliers, internal coordination between procurement, legal, and cybersecurity functions, and access to technical tools and supplier data. Organizational support is needed to enforce information requests and contractual obligations resulting from identified risks.
- **Cautions** Avoid overwhelming the program with excessive detail; focus on the most critical dependencies. Validate supplier-provided information and manage the sensitivity of the dependency map

as confidential business intelligence. Ensure the map is actively used to inform risk management and continuity plans, rather than treated as a static documentation exercise.

4.4.3 Integrate cybersecurity requirements into master supplier contracts

The outsourcing contract must explicitly include clauses that address cybersecurity requirements and risk management responsibilities. By embedding mandatory security provisions into the agreement, the organization ensures the vendor is legally bound to maintain a specified level of security, report incidents, and permit oversight. These clauses formalize the expectations for protecting the organization's data and services, making cybersecurity an enforceable part of the vendor's obligations. A well-structured contract sets clear performance standards and remedies, thereby mitigating risks throughout the supplier relationship. By creating a master contract requirement list you create a consistent basis. These requirements should be used as a condition for contract award, in the process of selecting suppliers.

- **Implementation** Before drafting or negotiating the contract, develop a set of baseline cybersecurity requirements that all vendors must adhere to. These should align with the organization's security policies and any regulatory obligations. Use these master requirements in the procurement process to assess and select potential suppliers.
  - **Collaborate with legal and security teams:** Ensure that both legal counsel and cybersecurity experts work together to craft the master requirement clauses. The legal team will ensure enforceability and clarity of language, while security experts ensure the technical appropriateness of the requirements.
  - **Description of service:** All outsourced services must be clearly documented, specifying each function and responsibility. Roles and responsibilities should be explicitly assigned to both the provider and client, clearly defining service boundaries, critical business functions, and any exclusions. Performance standards and service levels must be referenced clearly to set measurable expectations.
  - **Sub-outsourcing arrangements:** Providers should be required to notify and obtain prior written consent from the client for all subcontracting activities. An approved subcontractor list must be maintained, explicitly restricting sub-outsourcing of critical functions. Contractual requirements such as security, data protection, and service levels must flow down to subcontractors, with primary provider accountability and liability for subcontractor performance. Clients must have audit rights, receive regular subcontractor reports, and retain the right to object to high-risk subcontractors.
  - **Service and data locations:** Contractual clauses must specify permissible geographic locations for service delivery, data processing, and storage. Providers should seek advance client approval for any changes, particularly concerning critical functions. Clauses must align with data residency and cross-border transfer compliance requirements and include provisions for disaster recovery and contingency site locations.
  - **Information security:** Baseline and advanced security measures, referencing established standards such as ISO 27001 and NIST, must be clearly defined. It is recommended to adopt the same standards within both acquirer and supplier organizations where possible to enhance consistency in security practices, facilitate easier auditing, and fosters a mutual understanding of security expectations. Providers are obligated to maintain documented security policies, conduct regular security audits, ensure certification compliance, and implement robust incident response procedures, including mandatory reporting of security incidents. Providers must also assume liability and swiftly remediate security vulnerabilities or breaches.
  - **Data access, restoration, and return upon termination:** agreements on data access during and after contract termination must be established. Providers must regularly back up data, maintain restoration capabilities, and comply with detailed obligations regarding data return post-termination. Transition assistance, complete data deletion post-termination, and contingencies for provider insolvency must also be explicitly covered.
  - **Service level agreements (SLAs):** Clear, measurable KPIs must be established for service performance, including availability, response time, and resolution times. Reporting methodologies, regular SLA performance reviews, and enforceable remedies such as service credits and termination rights for breaches must be included. Stricter SLAs must apply to critical business functions, supported by frequent monitoring and audit rights.
  - **Incident planning and support:** Providers must immediately notify and fully cooperate

during operational or cybersecurity incidents. Active participation in joint incident management, incident response/contingency planning, and post-incident root cause analysis is mandatory. Providers must maintain continuous service continuity measures during incident resolution to mitigate business impacts.

- **Obligation to cooperate:** Providers must offer full cooperation during client audits, regulatory inspections, and risk assessments. This includes active information sharing, joint risk management activities, and ongoing collaborative efforts. Providers must commit to transparency, accountability, and mutual support, particularly to comply with regulatory obligations.
- **Termination rights and minimum notice periods:** Contracts must clearly define grounds for termination, including termination for cause, convenience, or regulatory directives, along with appropriate minimum notice periods. Cure periods for minor breaches and immediate termination rights for critical failures must be clearly outlined. The contract should also detail termination assistance obligations, transition planning, and continuity assurance measures.
- **Participation in awareness programs and training courses:** Providers must mandate their staff to participate in client-provided or approved cyber security and compliance training. Training frequency, attendance tracking, and certification compliance must be clearly stipulated. Training scope, associated costs, scheduling logistics, and language accessibility requirements must also be specified.
- **Specific clauses for critical suppliers:** Critical suppliers must adhere to enhanced contractual provisions explicitly addressing heightened cybersecurity risks. Specific clauses include mandatory advanced threat monitoring, stringent access control measures, dedicated security personnel, shorter incident response notification times, immediate termination rights for severe breaches, increased frequency of security audits, detailed business continuity and disaster recovery requirements, and the necessity for stringent approval procedures for any sub-outsourcing or data location changes. These clauses must ensure maximum operational resilience, rigorous risk mitigation, and comprehensive regulatory compliance for critical business functions

- **Objective** The objective is to comprehensively mitigate cybersecurity supply chain risks by clearly defining roles, responsibilities, performance standards, security obligations, and continuity provisions in outsourcing arrangements. This ensures accountability, operational resilience, regulatory compliance, and continuous improvement of security awareness across the entire outsourcing supply chain.
- **When to apply** This consolidated clause is critical for all outsourcing engagements involving sensitive data, critical business functions, regulated industries, or where third-party failures pose significant business risk. For lower-risk outsourcing, requirements may be scaled down appropriately, while critical functions demand stringent adherence to all detailed provisions. The master requirement list should be developed after a clear C-SCRM policy has been defined that outlines the internal security measures and risk appetite on which to build the contractual clauses.
- **Costs** Implementation entails upfront effort and potential increased operational costs due to compliance, auditing, and training requirements. These costs are justified through significant risk mitigation, reduced incident-related expenses, improved operational resilience, and regulatory compliance, resulting in long-term cost savings.
- **Prerequisite conditions** A thorough internal risk assessment, regulatory compliance review, clear exit strategy development, identification of business continuity needs, and vendor due diligence must precede implementation. Clear internal stakeholder alignment, contract negotiation transparency, and proactive vendor collaboration are essential prerequisites.
- **Cautions** Avoid ambiguous or overly rigid clauses to ensure flexibility and enforceability. Balance comprehensive requirements with practical operational capabilities. Regularly review and update contractual clauses to adapt to evolving risks and regulations. Ensure clarity in cost-sharing and clearly delineate provider versus client responsibilities to avoid disputes. Regular monitoring, joint risk reviews, and proactive management practices are crucial to ensuring ongoing compliance and effectiveness of these comprehensive contractual controls.

Chapter 5

Interview results

This chapter presents the empirical findings derived from a series of semi-structured interviews conducted with cybersecurity professionals. In total, eight interviews were conducted with experts from various domains including cyber strategy, governance, operational technology, and technical consulting. The participants had professional experience ranging from 1.5 to over 25 years, and held diverse roles such as policy officer, technical director, senior manager, and cybersecurity associate. These interviews were guided by a semi-structured protocol that explored perceptions of C-SCRM challenges, risk sources, current mitigation practices, and limitations of existing frameworks. Additionally, the developed best practice implementation guideline was presented to each expert for evaluation. Their perceptions were measured using a modified version of the FACE instrument, which captured feedback across key implementation dimensions: Priority, Feasibility, Acceptability, Cost, Equity, and Intent-to-Implement. This chapter reports the resulting codes and categories and distills key insights from the data.

5.1 Codes and categories

In total 102 codes were collected throughout the interviews. These codes were gathered following the grounded theory process [40] as discussed in Section 2.4.3. Table 5.1 presents the number of codes gathered after each individual interview.

Interview	Number of codes
1	70
2	39
3	46
4	51
5	64
6	73
7	42
8	62

Table 5.1: Number of codes collected per interview.

To eliminate double or similar codes, these codes are consolidated and translated into distinct concepts. The concepts are then organized into categories and subcategories. The complete set of distilled concepts and (sub-)categories can be found in Appendix D. The following section elaborates on the specific insights derived from these concepts.

5.2 Expert insights

Using the concepts and their (sub-)categories mentioned above, we can distill insights on the topic of C-SCRM. In this Section we will discuss the expert views on challenges, risks, sources of risks and measures in C-SCRM and their perspectives on the existing C-SCRM guidance documents. Sections 6.4.2 and 6.4.3

will discuss the insights from the interviews that reflect on the FACE scores and limitations of the best practice implementation guideline we developed.

5.2.1 Challenges and risks

A recurring theme in the interviews was the lack of clear ownership and accountability. Experts observed that no single function consistently owns third-party cyber risk, with departments like procurement, security, legal, and business units all having a stake. As one participant put it, C-SCRM within certain organizations becomes "like a jungle" with no single point of responsibility, leading to policy and process gaps. A related challenge is integrating C-SCRM across the organization. Even when security processes are initiated, they often remain isolated within certain departments, failing to align with the overall enterprise risk approach. As one expert explained, "they might have [C-SCRM] completely implemented, but it's operating in a silo and doesn't integrate with the broader picture. At the end of the day, what they're doing is kind of worthless."

Resource limitations further complicate C-SCRM efforts. Effective management requires skilled personnel, and many organizations lack the resources to implement comprehensive risk processes. One expert bluntly stated that third-party risk management "is always costly," emphasizing the need for dedicated time and staff to negotiate security clauses in supplier contracts. One interviewee noted, "a small business can have a complex supply chain but not enough people to resolve all of it," underscoring that limited manpower, budget, and knowledge are fundamental challenges.

The complexity of modern supply chains, especially with multiple subcontracting layers, further exacerbates C-SCRM. As one participant observed, companies struggle with "poor traceability" and "masked identities" of sub-suppliers. This makes it difficult to obtain accurate and timely information on supplier security postures, particularly beyond the first tier. The dynamic nature of supply chains, with constantly evolving vendor relationships and technologies, adds another layer of difficulty in maintaining up-to-date risk assessments. One expert emphasized that organizations might have "tens of thousands of third parties," yet can only "meaningfully care about a small fraction of them," highlighting the challenge of focusing efforts on the most critical risks due to limited resources.

Another major concern is scale: organizations are required to track thousands of suppliers, including fourth-tier vendors, and continuously assess their security. One participant described the task of checking the entire vendor landscape annually or ongoingly as "insane" without automation. While larger organizations struggle with this scale, smaller businesses face high dependency risks, as they often cannot easily replace critical vendors or enforce security requirements. This concern is particularly pressing as frameworks now emphasize operational resilience, such as having exit plans for suppliers.

Stakeholder misalignment adds another layer of complexity. Tensions between security teams, which prioritize rigorous supplier vetting, and procurement teams, focused on cost, speed, and supplier relationships, are common. One expert noted, "we do get weird pushback from... non-information security experts, [like] procurement people," reflecting how security requirements can disrupt vendor onboarding. To address this, several interviewees emphasized the importance of early and ongoing engagement with procurement and business owners to ensure that all concerns are considered. Without such collaboration, even well-designed programs may face internal resistance.

In conclusion, the implementation of C-SCRM is hindered by organizational silos, resource constraints, and the complex, dynamic nature of supply chains. Effective risk management requires clear ownership, cross-functional collaboration, and smarter tools to handle the scale and complexity of modern vendor networks.

5.2.2 Mitigation measures and best practices

To effectively address supply chain cybersecurity risks, organizations must adopt a structured, proactive approach built around several foundational practices. A recurring theme among experts is governance: creating a clear structure with executive support that brings together all relevant stakeholders: procurement, IT, security, risk, and legal. As one expert put it, "You need to mix all of the separate processes that exist now, because supply chain risk touches many domains and only a governance frame with the right people can make decisions stick." Others highlighted that new regulations like the EU's DORA are pushing boards to take direct responsibility for third-party ICT risks.

Another essential practice is to identify and categorize suppliers. Many organizations struggle to maintain even a basic inventory. As one participant noted, "Just getting a comprehensive list of suppliers is a challenge in itself for larger firms, but it is the prerequisite for everything else." Experts recommended triaging vendors through criticality or risk-tiering, focusing intense scrutiny on high-risk or high-impact suppliers, while applying proportionate controls to the rest. "You can only afford to meaningfully care about a small fraction of suppliers," one interviewee observed.

Once suppliers are categorized, assessments and due diligence follow. These typically include standardized questionnaires, documentation reviews, certifications like ISO 27001 or SOC 2 report, and sometimes audits. However, experts stressed that flexibility is essential. One expert gave a telling example of a niche supplier (a one-person company maintaining a critical database), "that would never fit the usual checklist" approach. Traditional measures (asking for an ISO 27001 certificate or a SOC 2 report) made no sense for a lone administrator, so bespoke controls (like supervising their access with specialized software) had to be devised.

This illustrated the need for flexibility: while industry best practices (ISO, NIST controls, etc.) provide a baseline, companies often must tailor requirements to the specific risk context of a supplier. Several interviewees said the core of C-SCRM is a robust vendor classification and assurance mechanism, wherein each tier of vendor has a defined set of required controls or audits, but with the ability to adjust for outliers.

The shift toward continuous monitoring was another major theme. Experts critiqued the limitations of annual audits "Running audits once a year and then being 8 months blind," as one participant described and endorsed real-time tools for tracking supplier security posture, detecting vulnerabilities, and responding rapidly. This includes monitoring news for breaches, requiring regular updates, and tracking key indicators.

Still, monitoring without action is insufficient. A strong message from practitioners was the need for remediation and enforcement. "Continuous monitoring is not enough... you have to engage with the vendor to find a way to get [issues] fixed, because if you never fix any of the issues you find then there's not a lot of value to what you're doing." Enforcement relies heavily on contracts, embedding clauses for standards compliance, audit rights, and breach notification.

As one expert put it, you sometimes have to "torture your vendor with audits" to drive improvement highlighting how audit rights can be strategically used as leverage in supplier relationships.

Security in procurement decisions also emerged as a lever. Some organizations score vendors on cybersecurity during RFPs, using security posture as a competitive factor. "You communicate it to the vendor: look, you lost this bid because your cybersecurity really didn't look good," said one expert, noting this incentivizes suppliers to improve. Yet this practice is indicated to not be widely adopted.

Finally, resilience and response planning is growing in importance. Organizations must assume supplier failures will occur and prepare accordingly. This includes embedding third-party scenarios into incident response plans and maintaining exit strategies for critical vendors. One expert warned, "Often there is no alternative choice for smaller organizations, there is a highly concentrated dependency on certain vendors." Regulators are increasingly mandating such strategies to ensure continuity.

In summary, effective C-SCRM depends on a layered and integrated approach:

- Governance structures and policies
- Supplier inventory and tiering
- Flexible but robust assessments
- Continuous monitoring and targeted enforcement
- Cybersecurity integrated into procurement
- Collaborative improvement and training
- Resilience through response planning and vendor exit strategies

No single measure is enough on its own. As experts emphasized, true supply chain risk management requires a combination of practices that create "defense in depth."

5.2.3 Limitations of existing C-SCRM guidance documents

Despite the abundance of C-SCRM frameworks such as ISO standards, NIST publications, and regulatory mandates like DORA; experts consistently voiced frustration with their practical limitations. While these documents offer high-level recommendations and comprehensive checklists, they often fall short where it matters most: operational guidance. "There is a plethora of guidance... but meaningful guidance that actually will meaningfully address the risks is very lacking."

This sentiment was echoed repeatedly. Experts noted that frameworks tend to state what should be done but provide little insight into how to achieve these tasks in real-world conditions. One practitioner pointed out the disconnect: "A standard might require that all contracts include security clauses and all vendors are risk-assessed, but it will not tell a company how to achieve this when contracts are scattered across departments and no central vendor list exists."

A recurring criticism was that most frameworks assume a level of organizational maturity and structure that many firms simply do not have. For instance, DORA requires firms to identify "critical" third parties, but one expert noted: "It's taken for granted an organization knows who their critical third parties are, and it's like, no actually that's probably the biggest challenge."

Frameworks also tend to ignore foundational steps like building supplier inventories, establishing governance structures, and securing cross-functional collaboration. As one interviewee put it: "There isn't a lot of information on how we should create... [a] collaborative environment," despite the fact that such collaboration is "the biggest thing that's needed".

Tailoring these generic frameworks to specific organizational contexts is another challenge. One participant remarked that a one-size-fits-all model simply doesn't work, especially when guidance is applied across drastically different sectors or organization sizes. Smaller companies, in particular, face unique barriers. One expert noted: "It's less costly... to just get it right the first time" with a simple, fresh approach than to retrofit a massive framework designed for large enterprises.

This gap between frameworks and applicability leads many organizations to cobble together their own interpretations, combining elements from ISO, NIST, sector regulations, and consulting advice. As one expert described: "You need to mix all of these [documents] to cover all areas." But this mixing is not always successful. Experts said supply chain risk management is often the lowest-scoring domain in client maturity assessments, not for lack of guidance, but because the guidance is "not easy to follow" and thus "not adopted at all."

A deeper issue highlighted by several experts is the lack of interdisciplinary expertise needed to implement C-SCRM effectively. Knowledge across technical risk, procurement, contracting, and vendor management is rarely found in one team: "Firms struggle with the lack of expertise in-house to do it sufficiently." This results in superficial, compliance-driven efforts "tick-box risk assessments", rather than real risk mitigation. One interviewee cautioned that without meaningful implementation: "EU regulatory compliance may force you to waste money on this [C-SCRM]" unless it actually improves security outcomes.

Frameworks also lag behind evolving threats and practices. They often fail to address emerging supply chain attack models or modern tools like continuous monitoring and shared assessments. One expert summarized: "The practices keep developing in the field, with smarter tools and techniques, but the formal standards don't take those into account... they remain neutral and static."

In sum, the most pressing issues with current C-SCRM guidance are:

- Overly high-level and abstract language lacking actionable steps
- Poor scalability and adaptability for smaller or less mature organizations
- Gaps in operationalization, including governance, remediation, and sustainability
- Fragmented and overlapping frameworks that require complex integration
- Outdated content that doesn't reflect current threats or tools
- Assumptions of internal capacity and expertise that many organizations lack

While some experts believe these frameworks can still drive value "if you interpret them in a very optimistic way" there's a strong consensus that without clear, tailored, and prioritized implementation guidance, their practical impact will remain limited.

5.2.4 FACE scoring

Table 5.2 present how the interview participants scored our newly developed implementation guideline using the FACE instrument [63]. Section 6.4 further interprets these scores and presents some of the practical feedback given by the participants to elaborate on the given scores.

Dimension	Question	Yes	Probably no	No	Varies	Don't know
Priority	Do you consider the lack of actionable guidance that lowers the expertise for establishing and operating a C-SCRM capability a priority issue within the field?	5	-	1	2	-
Feasibility	Would the implementation of the practices and recommendations outlined in the C-SCRM guideline be sustainable?	7	-	-	1	-
Acceptability	Do you feel the guideline would be acceptable to stakeholders involved in implementation?	7	-	-	1	-
Cost	Do you feel that implementation of the guideline would be costly to stakeholders?	-	1	4	3	-
Equity	Do you feel that implementation of the guideline would positively impact the inequity between organizations with differing resources and levels of cybersecurity maturity (e.g., SMEs vs. large enterprises)?	6	-	-	2	-
Intent-to-Implement	Based on your current understanding, would you intend to adopt or integrate the recommendations in this C-SCRM guideline into existing risk management practices?	8	-	-	-	-

Table 5.2: Overview of perception scoring by interview participants following the FACE instrument [63].

Chapter 6

Discussion

This chapter brings together the findings from the literature review, expert interviews, and the development of the C-SCRM implementation guideline to critically examine their significance, coherence, and implications. The goal is to synthesize the various strands of the research to evaluate how well the proposed guideline addresses the challenges identified in both academic and industry sources, and how it aligns with the practical needs expressed by experts. The discussion begins with a reflection on the limitations of existing academic and industry guidance, followed by an assessment of how the developed guideline compares to the requirements of the NIS2 Directive. Subsequently, the chapter reflects on the internal design and evaluation of the guideline itself, including expert feedback gathered through the FACE framework. This integrated analysis serves to highlight the contribution of the research, while also identifying areas for refinement and further exploration.

6.1 Academic literature evaluation

The body of academic literature on C-SCRM, as analyzed in Section 3.2, offers valuable information in this domain. However, it presents important gaps and shortcomings that deserve critical reflection. While the body of research provides useful frameworks, classifications of risk, and proposed countermeasures, our selection of articles tends to be limited in actionable recommendations that organizations can realistically implement.

6.1.1 Broad conceptual focus, limited practical application

All of the reviewed studies highlight the need for integrated, holistic approaches that combine technical, organizational, and inter-organizational aspects of C-SCRM. Articles frequently point out the weaknesses of siloed or reactive strategies, and emphasize the importance of proactive, organization-wide measures. However, while these papers make strong theoretical arguments, they often remain on a conceptual level without offering clear, hands-on guidance. For example, Boyson [15] calls for strategic control frameworks but offers limited operational detail. This makes it difficult for organizations to translate these academic insights into practical solutions, which paradoxically reinforces the disconnect between theory and practice that authors like Cheung et al. [17] and Colicchia et al. [18] themselves highlight.

6.1.2 Complexity and visibility: strong problem description, weak solutions

The literature is particularly effective at describing the challenges of supply chain complexity, lack of visibility across multiple tiers, and the risk of cascading failures. Authors such as Alanazi and Solangi [5] provide detailed typologies of supply chain complexity, while others stress the importance of improving transparency across supplier networks. However, when it comes to solutions, most papers stop at broad suggestions for enhanced monitoring or collaboration, without addressing how organizations, especially those with limited resources, can implement measures to achieve these goals. In addition, the tension between maintaining trust and enforcing verification in supplier relationships, while acknowledged (e.g. Collier and Sarkis [19]), remains largely unresolved.

6.1.3 Risk quantification remains underdeveloped

A recurring challenge in the literature is the quantification of cyber risks. Although some articles highlight the difficulty of measuring cyber risks in complex supply chains, they often suggest advanced methods such as Monte Carlo simulations or Bayesian analysis [58] without discussing their feasibility or effectiveness. In practice, these tools can be too expensive or complex to implement for smaller organizations. This raises questions about how realistic some of these recommendations are given the rising inequality in the cybersecurity domain across organizations [32].

6.1.4 Supplier collaboration and governance: theory vs. practice

Collaboration with suppliers, including due diligence, governance, and risk sharing agreements, is widely recognized as essential in the literature [47, 34]. However, the academic work does not offer remediation for real-world difficulties encountered in these activities, such as power imbalances, competitive pressures, and data-sharing reluctance. While the idea of adopting a zero-trust model is often mentioned, few papers explore handling the practical trade-offs this involves, such as higher costs or potential strains on supplier relationships.

6.1.5 Evolving threats demand adaptable responses, but solutions are vague

The literature consistently recognizes that cyber threats are evolving, and attackers are becoming more sophisticated, particularly in exploiting the emerging technologies like IoT and cloud systems. Although continuous monitoring and improvement are recommended in the literature [70], there is limited guidance on how organizations can embed adaptability into their day-to-day practices. There is still a lack of detail on how to build learning loops or integrate real-time threat intelligence into decision-making processes.

6.1.6 Human factors are acknowledged but not deeply addressed

While human elements such as employee errors, insider threats, and lack of security awareness are recognized as major risk factors, the literature offers limited suggestions on how to tackle these issues in a structured way. Most recommendations stop at general advice to improve awareness or provide training, without delving into how to effectively build a stronger security culture or motivate behavioral change. However, it is precisely these deeper insights that are needed to structure an effective strategy toward that end goal.

6.2 Industry resource evaluation

Although the reviewed industry resources differ in nature, goal, and main themes, the documents converge on the view that modern cybersecurity cannot ignore the supply chain. Based on our analysis of all industry resources and the insights collected through the expert-interviews we identified certain points in which these documents come up short in delivering adequate guidance for C-SCRM. This section discusses the limitations we observed in the NIST, ISO and DORA documents.

6.2.1 Usability versus scope

All industry resources emphasize that supply chain cybersecurity risks must be managed as part of an organization's overall risk management program. As discussed in Section 3.3 a clear theme across these sources is that C-SCRM must be holistic, rather than ad hoc. NIST, ISO and DORA each stress formal programs and policies, multidisciplinarity, and treatment of suppliers as integral to security and resilience of any organization.

However, this holistic approach comes with the issue of usability versus scope: the guidance is so comprehensive that implementing it can be daunting. NIST SP 800-161 Rev.1, for example, extends to hundreds of pages and covers dozens of topics; its checklists of technical and contractual measures are exhaustive [13]. While thoroughness is good, the expert interviews indicate that smaller or less-mature organizations may struggle to know where to start. In fact, the NIST case studies acknowledge this gap directly, noting that "less mature organizations are in need of further practical guidance and methods" [14].

6.2.2 Implementation burden and cost

As indicated in both the expert interviews and the 2025 cybersecurity outlook of the World Economic Forum [32] an SME typically lacks dedicated supply chain or security teams and resources to carry out hundreds of control recommendations. The guidance rarely prioritizes or phases actions, leaving firms to wade through the full list themselves. This raises concerns about implementation burden and cost. The DORA RTS 86 [28] attempts to introduce proportionality through simplified frameworks for smaller entities, but the baseline requirements remain quite detailed. What is "simplified" in a legal DORA context can still overwhelm a small organization.

6.2.3 Lack of concrete examples and metrics

Most documents provide qualitative best practices rather than quantitative measures. For instance, ISO 27002:2022 simply states that organizations should define "processes and procedures" for ICT supply-chain risk, but it offers no example of how to measure or audit their effectiveness [45]. NIST IR 8276 suggests practices such as mentoring suppliers and including them in incident plans, yet it does not quantify how to evaluate readiness [12]. NIST's own case study report explicitly calls out this weakness in the current C-SCRM climate by calling for "quantitative cyber supply chain risk analysis and metrics" and other practical tools [14]. As discovered during the expert interviews organizations adopting these resources have little guidance on which metrics to collect (e.g. reduction in vulnerability disclosures, time to recover after supplier incidents, etc.) or how to gauge adequate performance. This gap makes it hard to demonstrate ROI or improvement, which can undermine executive buy-in.

6.2.4 Integration and overlap among frameworks

In trying to cover all bases, the various guidances sometimes have overlapping or even conflicting directives. For example, IR 8276 encourages a collaborative relationship with suppliers (mentoring and joint resilience exercises) [12], whereas DORA's approach is more about contractual control and audit rights [27, 28]. An organization working under both might be unclear whether to prioritize cooperative improvements or strict compliance. Similarly, mapping ISO controls (high-level, principle-based) to NIST practices (detailed, process-oriented) can be nontrivial. Companies operating internationally may face the burden of satisfying multiple sets of requirements with little concrete guidance on harmonization. The DORA RTS themselves acknowledge this complexity, but the result remains intricate (the final reports run dozens of pages) [27, 28]. Thus, usability and adaptability are strained when a single organization must interpret and implement several frameworks in parallel.

6.3 Relation between the developed guideline and NIS2

In this section, we evaluate how the best-practice implementation guideline aligns with the NIS2 Directive's requirements on C-SCRM as described in Section 2.5. Each section below corresponds to a key NIS2 C-SCRM requirement and examines whether the guideline meets, partially meets, or falls short of that requirement. The analysis details how specific best practices from the guideline support compliance, identifies gaps or limitations, and provides recommendations for improvement.

6.3.1 Comprehensive risk assessment

NIS2 mandates that organizations conduct thorough risk assessments that include risks stemming from their supply chain. The directive requires a risk analysis of all relevant systems, and emphasizes assessing the cybersecurity practices of suppliers (including secure development procedures).The C-SCRM guideline fully addresses this through a multi-tiered assessment approach. It establishes that organizations must proactively identify and evaluate cybersecurity risks posed by third-party products and services, in line with NIS2's emphasis on supply chain risk analysis.

The guideline prescribes a formal multi-method assessment and monitoring program for suppliers (best practice 2.5). This includes initial risk vetting at onboarding and ongoing risk monitoring via continuous performance tracking, audits, and third-party assessments. By requiring suppliers to support their questionnaire responses with evidence (policies, certifications, audit reports) and by analyzing any "red flags" to update the supplier's risk rating, the guideline ensures a comprehensive risk assessment process

that is iterative and evidence-based. These measures correspond well to NIS2's call for systematic evaluation of supplier risks. Additionally, best practice 2.4 directs that all contractors be "thoroughly vetted and evaluated for security risks" as part of contracting, ensuring that risk assessment is embedded early in supplier engagement. Taken together, these practices meet the NIS2 requirement for comprehensive supply chain risk analysis by covering the full lifecycle: initial risk identification, continuous evaluation, and integration of findings into risk management decisions.

One potential gap that can occur during implementation of the guideline is the consideration of fourth-party risks (sub-suppliers), which is discussed in Section 9. While Recital 85 encourages entities to consider risks from other levels of suppliers beyond their direct contractors, the guideline focuses primarily on direct third parties. To fully align with the spirit of NIS2's comprehensive risk assessment, the guideline could explicitly recommend organizations to extend their risk assessment scope to critical sub-contractors of suppliers where feasible.

This includes cascading risk assessment requirements down the supply chain, requiring critical suppliers to identify and disclose their key sub-suppliers and attest to their security, so that risks in the extended supply chain can be assessed. Furthermore, Recital 90 encourages cooperative risk assessments, which leverage industry risk information sharing to identify systemic risks in common supplier dependencies. By broadening the scope in these ways, the guideline's foundation for risk assessment can be enhanced to address indirect supplier risks.

6.3.2 Supply chain security policies

NIS2 explicitly requires organizations to establish policies addressing supply chain cybersecurity. Article 21(2)(d) mandates "supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers" as a core component of cybersecurity risk management measures. The guideline directly supports this through the development of a dedicated C-SCRM policy. Best practice 1.4 calls for creating an overarching C-SCRM policy that formalizes procedures across the supplier lifecycle. This practice aligns with NIS2's requirement to have clear policies governing third-party cybersecurity.

The guideline's emphasis on policy is evident in best practice 1.4: *Develop and maintain a comprehensive C-SCRM policy*. It insists that C-SCRM procedures be "formalized to ensure consistent execution throughout the organization" via an overarching policy. The policy is to incorporate cybersecurity requirements "into every stage of a system and product lifecycle, from initial design... through decommissioning," ensuring that supply chain considerations are built in by design. In particular, the guideline enumerates specific procedures that the policy must include, such as governance structures, secure development practices, communication/reporting channels with suppliers, training programs, contractual standards, supplier monitoring, incident response plans, and continuous improvement mechanisms. By bundling these into a single policy document, the guideline mirrors NIS2's intent that entities have an integrated supply chain security policy. It also highlights the need to continuously update the policy as the program evolves, which helps ensure ongoing compliance with evolving regulatory expectations.

In summary, the guideline fully meets the NIS2 directive to implement supply chain security policies by prescribing a comprehensive policy framework that is endorsed by leadership and applied organization wide. However, despite the guideline's policy coverage being robust, implementers aiming to fully align their C-SCRM function with NIS2 should explicitly map their C-SCRM policy to NIS2 requirements to simply enhance clarity and compliance tracking.

6.3.3 Incident reporting and response

NIS2 requires entities not only to have incident handling capabilities, but also to report significant incidents to authorities. From a third-party risk perspective, incidents originating at or involving suppliers must be swiftly managed and reported. The guideline addresses incident response planning with suppliers in mind and briefly mention s the need to include regulatory entities in reporting procedures. Thus, the guideline meets NIS2's requirements on internal incident response processes involving third parties, while partially addressing the reporting obligations by establishes internal and external reporting channels.

The guideline introduces best practice 2.6: *Develop and regularly test supplier-focused incident response plans*, which directly speaks to NIS2's incident management expectations. It mandates that robust incident response (IR), disaster recovery (DR), and business continuity plans be developed for scenarios

involving suppliers and that these plans be regularly tested. This ensures that an organization can rapidly respond to and recover from incidents caused by or affecting third parties. Moreover, the guideline integrates supplier considerations into incident processes: for example, in defining roles (best practice 1.3), it explicitly includes "Security monitoring and incident response" as a responsibility spanning internal and external stakeholders

This means that when a supplier-related incident occurs, predefined roles and communication processes are in place to coordinate the response across organizational boundaries. Additionally, best practice 2.2 on communication and reporting mechanisms establishes clear channels between internal teams and vendors for cybersecurity issues, including "regular reporting of security incidents... to ensure transparency". This implies that the organization expects suppliers to report incidents to them in a timely manner, which is critical for fulfilling NIS2's broader incident awareness and reporting requirements. These guideline measures align well with NIS2's incident handling mandate by creating a coordinated response framework that encompasses third-party incidents.

6.3.4 Continuous monitoring and evaluation

NIS2 envisions cybersecurity risk management as an ongoing process. Entities must continuously monitor their risk environment and the effectiveness of their security measures (Article 21(2)(f) calls for policies to assess the effectiveness of cybersecurity measures, which by extension includes supplier oversight). The guideline strongly emphasizes continuous monitoring and periodic re-evaluation of third-party risks, which aligns with these requirements. In Recital 85, NIS2 even suggests encouraging continuous diligence on suppliers and periodic assessments of their cybersecurity practices. The best-practice guideline meets this by establishing a comprehensive supplier monitoring framework with multiple feedback loops for regular evaluation.

Best practice 2.5: *Establish a comprehensive monitoring and assessment framework for suppliers*, is the cornerstone of continuous evaluation. The guideline stresses using multiple techniques to maintain ongoing visibility into the security, resilience, and compliance posture of external suppliers. Concretely, it recommends a combination of continuous monitoring tools (e.g., third-party risk rating services, real-time security feeds) and periodic assessments such as annual audits, certification checks, and on-site visits.

At the same time, they conduct scheduled reassessments: issuing updated questionnaires "periodically... to critical and high-risk third parties" and requiring evidence for controls, rather than mere self-attestation. The guideline also insists on systematically analyzing assessment results and feeding any deficiencies back into the risk management process (updating risk ratings and adjusting monitoring plans accordingly).

Furthermore, the policy framework (from best practice 1.4) includes "continuous improvement" procedures. This entails that the organization must regularly review and improve its cybersecurity practices and risk strategies, with "regular audits, assessments, and feedback loops" to drive ongoing enhancements. Collectively, these practices ensure that third-party risk management is not a one-time effort but a continual cycle, fully reflecting the NIS2 principle of continuous risk monitoring and iterative improvement.

The guideline's provisions for continuous monitoring are thorough, for full allignment with NIS2 implementers should explicitly adopt the proportionality principle in NIS2 (Recital 82) in their procedures, risk-based scaling of continuous monitoring (e.g., continuous real-time monitoring for the most critical suppliers, and at least quarterly or annual reviews for lower-risk suppliers).

6.3.5 Documentation and Auditability

NIS2 expects organizations to document their cybersecurity measures and be able to demonstrate compliance. For instance, Article 24 empowers authorities to supervise and request evidence of risk management practices. Having a clear audit trail and documentation of supply chain risk management activities is crucial. The best practice guideline explicitly stresses documentation and the importance of auditability for accountability and improvement, aligning well with NIS2's requirements for demonstrable compliance.

Throughout the guideline, there is an emphasis on creating and maintaining documentation as part of the C-SCRM program. Best practice 1.4 not only calls for formalizing procedures in writing, but also for

recording key governance decisions and structures in that policy (e.g., documenting the charter of the risk council, defined roles and processes as per best practices 1.1–1.3). This ensures that the organizational setup for managing third-party risk is transparent and referenceable.

Moreover, in best practice 2.1, the guideline cautions that "maintaining comprehensive documentation and reporting on C-SCRM activities is essential for accountability and continuous improvement". This statement underlines that every security requirement integrated into the lifecycle and every risk management action taken should be documented. The continuous improvement practice (2.7) also implies documentation via feedback loops and regular audits.

Together, these practices mean that an organization following the guideline will generate a robust paper trail: policies, risk assessment reports, supplier performance reviews, incident post-mortems, meeting minutes of the risk council, training attendance records, and so forth. All these can be shown to auditors or regulators to demonstrate NIS2 compliance. Importantly, the guideline also integrates auditability into contracts (e.g., requiring suppliers to provide evidence like audit reports during assessments) and into monitoring (e.g., verifying certifications). This layered approach to documentation meets NIS2's expectations that entities prove they have taken appropriate measures.

6.3.6 Contractual obligations on suppliers

NIS2, particularly in Recital 85, encourages organizations to "incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers". While the directive stops short of listing specific contract clauses, the expectation is that contracts with third parties will include provisions to manage security (such as requiring certain security standards, audit rights, incident notification, etc.). The C-SCRM guideline very clearly advocates embedding security requirements into supplier contracts, fully aligning with this aspect of NIS2.

Best practice 2.4: *Embed C-SCRM requirements into the supplier contracting lifecycle*, directly addresses contractual obligations. The guideline insists that any supplier providing critical services or products must adhere to the organization's cybersecurity standards and practices, as outlined in the C-SCRM policy.

Practically, this means security requirements are written into contracts and procurement processes. For example, the guideline's policy checklist explicitly notes that contracts should include clauses allowing for security vetting and ongoing compliance checks.

Moreover, the guideline suggests including obligations for suppliers to participate in the security program: in the training practice, it even mentions incorporating clauses requiring critical suppliers to maintain equivalent standards of cybersecurity awareness and training for their staff. This is a concrete example of a contractual obligation flowing down to the supplier. Additionally, the monitoring best practice (2.5) benefits from contracts that provide for audits and continuous monitoring. The guideline expects suppliers to comply by providing evidence and access for assessments.

All these points illustrate how the guideline operationalizes NIS2's call for supplier accountability via contracts: by embedding specific security requirements (compliance with policies, incident reporting duties, audit rights, etc.) into the supplier relationship from the outset. This approach meets NIS2's requirements and even provides a level of detail that Recital 85 implies but does not detail.

6.3.7 Management responsibility

NIS2 places accountability for cybersecurity on senior management. Article 20 ("Governance") requires that "management bodies of essential and important entities approve the cybersecurity risk-management measures" and oversee their implementation.It also implies that management must be knowledgeable about these measures. The best-practice guideline strongly reflects this principle by establishing executive engagement and oversight as a fundamental pillar of the C-SCRM program. It ensures that top management is not only aware of supply chain cybersecurity risks but actively involved in governance, thus aligning closely with NIS2's management responsibility mandate.

The entire Governance category (practices 1.1 through 1.3) is aimed at embedding C-SCRM into the organizational governance structure with leadership support. Best practice 1.2, "Strengthen board oversight and engagement in C-SCRM," directly speaks to management responsibility. It calls for regular

executive engagement by establishing formal reporting structures to the board and requiring management to receive updates on supply chain risk status and program effectiveness.

Specifically, the guideline advises creating a charter that defines how often and in what form the C-SCRM council or program reports to the management body. It also suggests scheduling regular board presentations (e.g. quarterly/annually) on key supplier risks and mitigation performance. This echoes NIS2's requirement that management approve and stay informed on cybersecurity measures.

Furthermore, best practice 1.1 sets up a cross-functional supply chain risk council with executive membership, ensuring that senior leaders from various departments (IT, security, procurement, etc.) are collectively responsible for supply chain risk decisions. This council concept "with leadership support and clear roles and responsibilities" institutionalizes management oversight from the start. The guideline's tone makes it clear that "leadership buy-in" is critical and that the "tone from the top" must prioritize supply chain security.

Additionally, through best practice 1.3, the guideline defines roles that likely include executive roles like a CISO or risk executive overseeing the program. The presence of these governance structures and the explicit strengthening of board engagement demonstrate that the guideline fully meets NIS2's intent to hold management accountable. In particular, the guideline also indirectly covers the NIS2 expectation of management cybersecurity knowledge by involving the board in regular discussions and requiring their understanding and input, it effectively ensures management is educated on cybersecurity matters.

The alignment here is strong. A possible gap is that NIS2 (Article 20) could hold individual executives liable for non-compliance, but the guideline doesn't explicitly discuss accountability or liability. To reinforce alignment formal approval and sign-off by the board or top management on major C-SCRM decisions is needed.

6.3.8 Training and collaboration

NIS2 underscores the importance of cybersecurity awareness and training in Article 21(2). It also encourages cooperation and information sharing, although mostly among Member States and at sector level (Recital 90), it stands to reason that organizations should collaborate with their suppliers on risk management. The guideline meets the training requirement through a dedicated best practice for role-based training and awareness, and it fosters collaboration both internally (cross-department) and externally (with suppliers), thereby aligning with the spirit of NIS2's emphasis on knowledge and cooperation in cybersecurity.

Best practice 2.3: *Implement role-based training and supply chain cybersecurity awareness*, directly fulfills the training aspect. The guideline calls for a comprehensive training and awareness program focused on supply chain cybersecurity risks for all relevant personnel. It explicitly mentions "all relevant personnel including executives, technical staff, and procurement officers" should understand supply chain threats and their role in managing these risks. This aligns perfectly with NIS2's requirement that staff (and notably management bodies) be trained in cybersecurity. The guideline further extends training to third parties: it recommends "regular cybersecurity training and awareness programs... for all employees and third-party vendors" to ensure they are informed of threats and best practices. Including suppliers in awareness efforts is a best practice that goes beyond NIS2's minimum and helps create a security culture across the supply chain.

On the collaboration side, the guideline's governance best practices (1.1 and 1.3) establish structures for collaboration. The cross-functional risk council brings together different internal stakeholders (IT, security, procurement, legal, etc.) to collaborate on supply chain risk decisions. This ensures silos are broken down internally. Practice 1.3 goes further by institutionalizing collaborative roles, structures, and processes that include external stakeholders like suppliers' security contacts. It suggests creating working groups and communication processes that involve both internal teams and external partners. Concretely, the guideline advises holding "joint post-incident reviews" with suppliers and even "annual conferences to discuss developments in the threat landscape" between the organization and its vendors. It also prescribes "regular meetings, shared dashboards, and established escalation procedures... including both internal and external communication" to facilitate information sharing. These elements resonate with NIS2's collaborative ethos (e.g., Recital 85's emphasis on relationships with suppliers).

While NIS2 doesn't mandate specific collaboration activities with vendors, the guideline's measures help ensure that the entity and its suppliers work together on cybersecurity (for example, by sharing

vulnerability information or coordinating on incident response), which can be seen as implementing NIS2's supply chain security requirement in practice.

6.3.9 Fourth-party risk

NIS2 recognizes that risks can propagate through complex supply chains. While the directive's requirements explicitly mention direct suppliers, Recital 85 notes that entities "could consider risks stemming from other levels of suppliers and service providers". This refers to fourth-party risk: the risk posed by the subcontractors and supply chain of your third-party suppliers.

The best practice guideline touches on this concept indirectly by holding primary suppliers to high standards and encouraging them to maintain secure practices, a register of all sub-outsourcing activities, and flow down requirements to critical sub-contractors. However, there is no specific best-practice dedicated to explicitly address how to manage fourth-party or Nth-tier risks.

Therefore, implementers aiming to achieve NIS2 compliance will need to expand best practice 4.2 and 4.3 to include risk assessments of fourth-parties. Best practice 4.3 requires suppliers to document an inventory of critical sub-suppliers. Based on this inventory conduct risk assessments on the sub-suppliers or require the supplier to execute these assessments based on agreed methods.

6.3.10 Conclusion

Overall, the analysis finds that the best-practice C-SCRM guideline is well-aligned with NIS2's TPRM requirements, with strengths in its structured, holistic approach that often exceed the Directive's baseline.

It excels in translating high-level NIS2 mandates into actionable controls and processes: for instance, it not only requires to "monitor supply chain risk" (as NIS2 does) but actually details how (through questionnaires, continuous monitoring tools, etc.). This actionable detail is a key strength, providing organizations a clear path to compliance.

Additionally, the guideline's focus on governance and culture (e.g., risk council, executive buy-in, training) addresses the often intangible aspects of NIS2 compliance, ensuring that third-party risk management is not just a checklist but an integrated organizational practice.

The areas where implementers would need additional alignment with the directive are relatively minor and largely involve making the implicit explicit. For example, formally incorporating regulatory incident reporting into incident response plans, or extending existing practices to cover fourth-party scenarios. These enhancements would ensure no gaps when an organization's C-SCRM program is scrutinized under NIS2's provisions. It is also recommended that organizations document a clear mapping between the policy created through best practice 1.4 and NIS2 articles/recitals to demonstrate compliance easily during audits or supervisory requests.

In conclusion, an organization implementing the best-practice C-SCRM guideline should be well-positioned to meet the NIS2 Directive's requirements for third-party cyber risk management. The guideline provides a strong foundation of controls and processes; with the recommended refinements, it can serve as a framework that not only achieves regulatory compliance but genuinely reduces supply chain cyber risk.

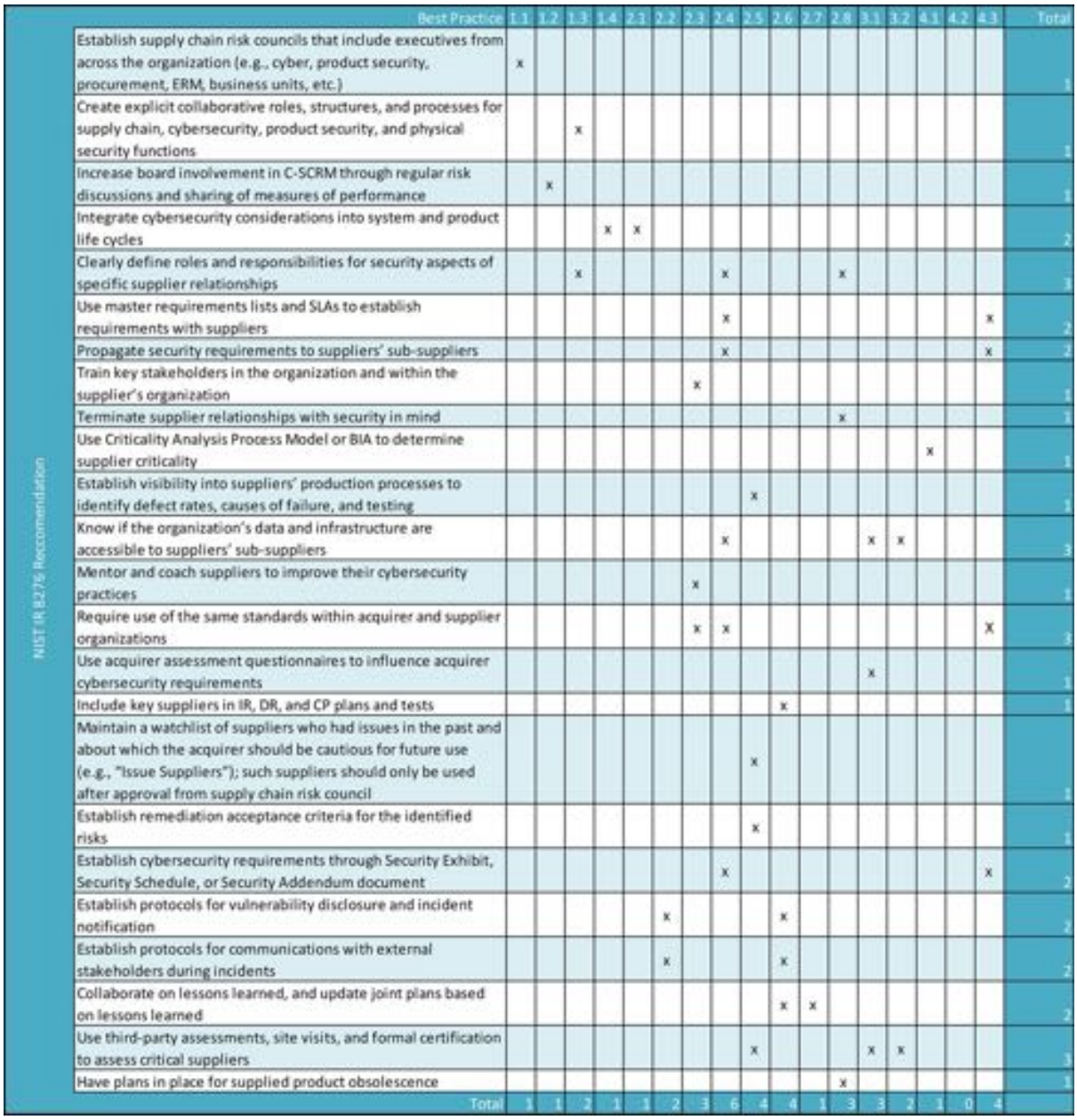
6.4 Guideline reflection

This section critically considers the underlying design choices, the methodological alignment with expert insights, and how the FACE evaluation results informed the perceived practicality and value of the guideline.

6.4.1 Design choices

The structure of our best practice implementation guideline has fundamental roots in the recommendation provided by NIST IR 8276 [12]. Figure 6.1 illustrates how each of the 24 recommendations is mapped to our best practices. By combining this mapping with the mapping between the recommendations and industry resources from Figure 3.5, we create a traceable trail from the data we collected in our industry resources analysis to our final guideline. Noticeable from the mapping in Figure 6.1 is the fact that best practice 4.2 does not feature a direct mapping to one of the recommendations.We decided

to include this best practice to form a bridge between the inventorization and prioritization of suppliers and the creation of an integrated overview of the full supply chain to start monitoring activities.



NIST IR 8276 Recommendation	Best Practice	1.1	1.2	1.3	1.4	2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	3.1	3.2	4.1	4.2	4.3	Total
	Establish supply chain risk councils that include executives from across the organization (e.g., cyber, product security, procurement, ERM, business units, etc.)	x																	1
	Create explicit collaborative roles, structures, and processes for supply chain, cybersecurity, product security, and physical security functions			x															1
	Increase board involvement in C-SCRM through regular risk discussions and sharing of measures of performance		x																1
	Integrate cybersecurity considerations into system and product life cycles				x	x													2
	Clearly define roles and responsibilities for security aspects of specific supplier relationships			x					x				x						3
	Use master requirements lists and SLAs to establish requirements with suppliers								x									x	2
	Propagate security requirements to suppliers' sub-suppliers								x									x	2
	Train key stakeholders in the organization and within the supplier's organization							x											1
	Terminate supplier relationships with security in mind												x						1
	Use Criticality Analysis Process Model or BIA to determine supplier criticality															x			1
	Establish visibility into suppliers' production processes to identify defect rates, causes of failure, and testing									x									1
	Know if the organization's data and infrastructure are accessible to suppliers' sub-suppliers								x					x	x				3
	Mentor and coach suppliers to improve their cybersecurity practices							x											1
	Require use of the same standards within acquirer and supplier organizations							x	x									x	3
	Use acquirer assessment questionnaires to influence acquirer cybersecurity requirements													x					1
	Include key suppliers in IR, DR, and CP plans and tests										x								1
	Maintain a watchlist of suppliers who had issues in the past and about which the acquirer should be cautious for future use (e.g., "Issue Suppliers"); such suppliers should only be used after approval from supply chain risk council									x									1
	Establish remediation acceptance criteria for the identified risks									x									1
	Establish cybersecurity requirements through Security Exhibit, Security Schedule, or Security Addendum document								x									x	2
	Establish protocols for vulnerability disclosure and incident notification						x				x								2
	Establish protocols for communications with external stakeholders during incidents						x				x								2
	Collaborate on lessons learned, and update joint plans based on lessons learned										x	x							2
	Use third-party assessments, site visits, and formal certification to assess critical suppliers									x				x	x				3
	Have plans in place for supplied product obsolescence												x						1
	Total	1	1	2	1	1	2	3	6	4	4	1	3	3	2	1	0	4	

Figure 6.1: Mapping between the 24 recommendations of NIST 8276 and our best practices

To establish the same level of traceability for the academic resources we analyzed, Figure 6.2 provides a mapping between the C-SCRM measures we identified in Section 3.2 and the best practices of our guideline where they have been adopted. This mapping shows that blockchain technology is the only measure not incorporated into our guideline. Blockchain is cited as a possible tool for improving supply chain integrity and traceability [41, 17]. Nevertheless, it was not incorporated into our final guideline. This decision is grounded in several key considerations.

First, none of the industry resources used in this research highlight blockchain as a recommended or feasible C-SCRM measure. Second, blockchain implementation is inherently resource-intensive both in terms of financial investment and required technical expertise [17].

For many smaller organizations, adopting blockchain technologies would require significant restructuring of digital infrastructure, training, and coordination among supply chain partners. Including such a measure would conflict with the very purpose of this guideline to make C-SCRM implementation attainable

for organizations with limited capacity. The same considerations apply for other advanced methods such as Monte Carlo simulations or Bayesian analysis as suggested by Pandey et al. [58].

Best practice 2.8 does not incorporate any of the measures from the academic literature. This best practice outlines needed procedures for supplier off-boarding and the planning of the obsolescence of products and services. It is notable that this theme does not hold a prominent place in the academic literature as a needed measure. While covering the entire lifecycle of a product or service and implementing a holistic approach is indicated as a challenge for a lot of organizations, the existing academic articles do not offer insights on how to implement an exit strategy in practice.

Figure 6.2: Mapping between the measures identified from academic literature and the best practices in which they are adopted.

6.4.2 FACE interpretation

The newly developed C-SCRM guideline was met with strong endorsement from experts, who praised its clarity, completeness, and practical value. They saw it not as a novel theory, but a coherent consolidation of best practices aligned with industry realities. As one expert put it, "It captures basically how to do it... it's in line with what's needed in the industry." Another affirmed, "This is the most complete and simple thing... I will definitely get value from it."

Feasibility

Experts overwhelmingly found the guideline feasible, especially because it mirrors existing organizational structures and emphasizes a phased, risk-based approach. "Definitely makes sense... it's connected with a lot of what we talked about," said one interviewee. Many noted its strength lies in consolidating scattered practices into a digestible format, enabling even smaller organizations to implement C-SCRM more effectively. However, feasibility hinges on focusing on critical areas: "You have to be organized about what we care about and why, that's the major obstacle here." Trying to apply all practices indiscriminately could be overwhelming, but a scoped, prioritized rollout was seen as sustainable.

Acceptability

The guideline was broadly acceptable across stakeholder groups, particularly because it integrates cross-functional concerns. "Information-security people would totally be on board," one expert said, but noted that buy-in from procurement and business units depends on how well their goals are reflected. Acceptance improves when the guideline is positioned as an enabler, helping avoid disruptions, not slowing procurement. One expert explained, "If procurement understands the process helps them avoid surprises and respects their objectives, they'll support it." The emphasis on integrated governance and early involvement of all functions was seen as critical to success.

Cost

Cost was recognized as a factor, but not a barrier. One participant noted that "[C-SCRM] is always costly," yet most experts argued that the guideline could optimize spending by focusing attention where it matters most. "If you have such a guideline, the implementation would be less costly because you know where to put your attention," said one. While some steps like improving contracts or hiring dedicated roles incur costs, these were viewed as necessary and worthwhile. A participant working with smaller firms said the guideline could even reduce costs by eliminating the excesive need for consulting since is eliminates the need to "check all different kinds of standards".

Equity

Experts agreed the guideline could help close the gap between large and small organizations. "100% yes," one said, noting SMEs could follow the roadmap without attending "expensive communities" or relying on costly consultants. It provides structure where smaller firms typically struggle due to lack of knowledge. Yet, there was realism about the enduring resource gap: "They will never have enough resources to be as thorough as a big company... that inequity will never go away." Still, by raising the baseline, the guideline offers "a fighting chance" to smaller players, and even prompts larger ones to streamline their often bloated processes.

Intent to implement

All experts expressed intent to adopt or recommend the guideline. They saw clear value in its completeness and simplicity. "I will definitely get value of it and adopt those things... because this is the most complete and simple thing" said one; another emphasized its practical utility, saying it gives a roadmap to present to leadership. The fact that the guideline reflects a consensus among different documentation boosted confidence: it's not one person's view, but a curated synthesis. Even the more skeptical participants saw it as adaptable and useful. Stating that it offers great possibilities to incorporate into existing toolkits.

6.4.3 Guideline limitations

Although the guideline was met with strong expert endorsement for its clarity and practical value in the preceding analysis, it is not without room for improvement.

Generalized best-practice approach and need for tailoring

One fundamental limitation of the guideline is its generalized, one-size-fits-all nature. By design, the best-practice recommendations provide a broad pathway intended to suit any industry or organization. While this makes the guideline widely applicable, it also means specific contextual nuances are not addressed.

Best practices in this context do have certain disadvantages that we have to be aware of [60]. First, our proposed best practices guideline offers a generalized pathway that is applicable across industries and sectors. This means that organizations should tailor the practical implications of this guideline to their own needs and not blindly take them at face value. "What is a best practice for some is not so for others" [60].

In other words, the guideline's broad scope necessitates tailoring in practice, organizations must interpret and adapt the steps to their own environment rather than implement them verbatim. This was echoed in the interviews, where experts stressed that blindly following "best practices" can be misguided if a company's size, sector, or risk profile calls for a different approach. The generalized format, while a strength in offering a common foundation, is a limitation in that it does not provide explicit, sector-specific guidance. Practitioners are left to bridge the gap between the guideline's universal advice and the unique demands of their business context.

This reliance on user interpretation can lead to inconsistent outcomes, underscoring that the guideline is not a plug-and-play solution. It needs to be complemented with organization-specific judgement, which smaller firms or less experienced teams might still struggle with despite the "best practice" label. The intent is for the guideline to raise the baseline, but how each organization gets there will differ, a nuance the guideline itself does not elaborate, apart from a general warning that adaptation is necessary. This limitation suggests that additional support (e.g. industry-specific examples or decision trees) would be beneficial to help practitioners customize the guidance effectively.

Insufficient guidance on business impact analysis and prioritization

Another significant gap identified by the experts is the lack of concrete guidance on conducting Business Impact Analyses (BIA) for suppliers and prioritizing third parties based on criticality. The guideline does advise organizations to "identify and prioritize suppliers" (and hints at considering business impact, stability, etc.), but it remains abstract on the methodology for doing so. Interviewees found this problematic, as determining the business impact of a supplier is considered "one of the golden questions ... and everyone does it differently".

In the current guideline, the criteria for prioritization are listed (e.g. impact of supplier failure, availability of alternatives, etc.), yet no standardized approach or formula is offered for how to weigh or calculate these factors in practice. One expert noted that the "how to do it can be a little bit hidden", meaning the guideline tells what to consider (e.g. conduct a business impact study) but not how to execute it in a consistent way.

The absence of a defined BIA process leaves practitioners uncertain. For instance, should they use quantitative scoring, tier suppliers by criticality qualitatively, or perform full business continuity impact assessments for each vendor? Several experts suggested that providing at least a basic template or example for BIA would enhance the guideline's practicality. Without such guidance, organizations might default to simplistic proxies (like contract value or spend) for prioritization, which may not truly reflect business criticality. Indeed, one interviewee indicated that different companies currently prioritize "maybe just [by] contract value" or only by perceived operational impact, due to lack of a clear model.

The risk here is inconsistency: two firms following the same guideline could end up with very different supplier rankings if left to devise their own impact analyses. In summary, the expert feedback reveals that the guideline's treatment of BIA is too high-level, representing a practical limitation. Practitioners still need more step-by-step direction on how to perform a BIA for third-party services. For example, how to quantify potential losses or disruption if a given supplier fails, and how to assign scores or tiers based on those findings. Making this process more explicit and standardized (at least in example form) was seen as crucial for ensuring the guideline can be implemented uniformly and effectively across organizations.

Challenges in managing change and legacy backlogs

Experts also pointed out that the guideline does not address the pragmatic challenge of managing change over time, particularly the scenario of dealing with an existing backlog of suppliers and contracts. The implementation steps are presented as if an organization can start fresh, moving forward with improved practices, but interviewees stressed that real organizations must retrofit these practices to an existing supplier base. One participant highlighted this by asking whether the guideline differentiates between "looking forward" (i.e. new contracts and assessments going ahead) and "cleaning the backlog" of existing

agreements In practice, no company has the luxury of focusing only on new suppliers; as the expert bluntly put it, "in the entire world there is no organization that can focus on the future [only]... I have thousands of contracts to handle now".

This reflects a limitation: the guideline lacks explicit guidance on how to apply its recommendations to suppliers already onboarded or contracts already in place. For example, if an enterprise has never performed systematic supplier risk assessments, the guideline doesn't say how to catch up, should they assess all current vendors immediately, or phase it in? Likewise, if contracts with key suppliers lack the recommended cybersecurity clauses, the guideline is silent on how to update or renegotiate those in practice. Interviewees found this omission significant, because implementing C-SCRM is often a change management exercise that involves going back to remediate past gaps.

Without advice here, organizations might feel overwhelmed. Experts suggested including a phased approach for backlog reduction. For instance, "for the first year, make sure that you cover all the critical [suppliers]" before moving on to less critical ones later. Such guidance would help practitioners prioritize and sequence the work on legacy suppliers. Similarly, making a clear distinction between processes for new onboarding versus retrofit of existing contracts would enhance practicality.

The absence of these instructions is a limitation that could impede implementation: firms may delay action on the hardest part (addressing the backlog of hundreds of unchecked vendors) or proceed ad-hoc, whereas a structured backlog reduction plan (focus on top X suppliers per quarter, etc.) is what experts felt was "amazing guidance" still needed. In summary, the guideline in its current form assumes a greenfield implementation, whereas experts noted that most organizations must integrate these practices into an established, sometimes sprawling, supplier landscape. The change management aspects, how to get organizational buy-in, handle the surge of workload, and systematically work through existing gaps, are not covered, marking a practical shortcoming of the guideline from an implementation standpoint.

Ambiguity in supplier register contents and maintenance

The supplier register (or inventory of suppliers) is a foundational element in the guideline, yet experts found the guidance around it to be lacking in specificity. The guideline advises creating and maintaining a register of all critical suppliers, but it does not clearly delineate what information that register should contain or how detailed it should be.

This is a limitation for implementation: without clear direction, one organization's supplier register might simply be a list of company names, while another's might include contacts, contract values, risk scores, business criticality, last assessment date, etc. The experts indicated that more concrete guidance here would be valuable. For example, the guideline could have stated that each supplier entry should include fields such as the supplier's criticality tier, the products/services they provide, any regulatory or data access implications, date of last risk assessment, outstanding issues or remediation plans, and so on.

In the interviews, practitioners implied that a well-defined supplier register is key to managing C-SCRM, and they expected the guideline to provide a model or template for it. The lack of such detail means organizations must develop their own structure for the register, potentially missing important attributes.

Another related point is the maintenance of the supplier register: the guideline encourages keeping it updated but gives no practical tips on how to achieve this (e.g. via periodic reviews, integration with procurement systems, or assigning ownership to a specific role). The interviews did not explicitly mention maintenance procedures, but by highlighting uncertainty about content, it is clear that defining the process and content for the register is an area where practitioners need more help.

In summary, the guideline's treatment of the supplier register is high-level, and this ambiguity is a limitation for implementation. Experts felt that organizations would benefit from more explicit instructions on what belongs in the register and how to use it as a living tool for C-SCRM (for instance, leveraging it to trigger assessments or as input for business impact analysis). Without that, the register could remain an underutilized checklist item rather than a robust risk management resource.

Conducting assurance reviews and third-party audits in practice

Experts further identified a limitation in how the guideline handles supplier assurance and audit artifacts (such as certification reports, audit attestations, or SOC 2 report). The guideline encourages relying

on “verified verifications”, essentially using third-party certifications or audits to gain confidence in a supplier’s security posture, but it gives little advice on what to do with those documents next. Several interviewees stressed that obtaining an audit report is only the first step; the real challenge is interpreting its contents and acting on them. One participant put it plainly: “Reading those assurance reports is a thing. How to evaluate those reports? ... Even if you have a SOC 2 report in your hand, somebody needs to check whether it is satisfactory or not”.

In its current form, the guideline does not describe how to perform such an evaluation. This is a practical shortcoming because many organizations, especially those new to C-SCRM, may not know how to glean actionable findings from a vendor’s ISO 27001 certificate or SOC report. The experts implied that the guideline could improve by outlining, for example, what sections of a SOC 2 report to look at (scope, findings, auditor’s opinion, exceptions noted, etc.), how to verify the certification’s validity and coverage, and how to follow up on any gaps.

Without this, there’s a risk that practitioners will check the box by collecting assurance documents but not fully understand their implications – potentially missing warning signs that were buried in an audit report’s fine print. Additionally, one interviewee brainstormed whether the guideline’s “rely on certifications” advice covers which aspects to verify on those certifications.

This suggests that beyond reading reports, practitioners want guidance on validating certificates (e.g. confirming a cloud provider’s compliance certificate actually covers the services they use, or that a penetration test report is recent and relevant). The lack of clarity on assurance review procedures means organizations must develop their own approach to evaluating third-party attestations. This could lead to inconsistent rigor, some might over-rely on any certificate as a clean bill of health, while others might duplicate effort by re-assessing even certified suppliers from scratch, neither of which is ideal.

In summary, the interviews revealed that the guideline’s treatment of third-party assurance is incomplete. To be truly implementable, it should not only tell organizations to collect assurance evidence, but also guide them in how to critically review and trust (or distrust) that evidence. The current omission of review techniques is therefore a noteworthy limitation, leaving a knowledge gap for practitioners who must make judgment calls about suppliers’ security claims.

Lack of defined KPIs for supplier performance monitoring

Closely related to assurance and oversight is the guideline’s omission of specific Key Performance Indicators (KPIs) or metrics for ongoing supplier risk management. The guideline certainly emphasizes monitoring and periodic reviews of suppliers, but experts noted it stops short of saying which performance or risk indicators to actually monitor.

During the interviews, one participant explicitly pointed out that the section on periodic contract reviews could be strengthened by incorporating KPIs, to ensure those reviews include measurable performance checks.

In practice, contract or supplier performance reviews should track things like the supplier’s adherence to SLAs, incident history, outstanding vulnerabilities or non-compliances, and so forth. However, the guideline currently provides no examples of such metrics. This is a limitation because defining KPIs is critical for translating a high-level review into tangible oversight. Without guidance, organizations might struggle to identify whether their supplier risk posture is improving or deteriorating over time.

The experts indicated that regulators, expect firms to monitor supplier performance, which implicitly calls for metrics, yet the guideline doesn’t link its recommendations to any quantifiable indicators. An organization implementing the guideline might wonder: should we measure the number of suppliers without recent risk assessments? The percentage of critical suppliers with up-to-date certifications? The time suppliers take to remediate identified issues? These are the kind of practical questions left unanswered.

The absence of KPIs also makes it harder to demonstrate the value or progress of C-SCRM activities to management, a point practitioners implicitly care about. The interview feedback strongly suggests adding at least a sample set of KPIs or key risk indicators associated with each phase (e.g., “% of high-risk suppliers with risk treatment plans in place” or “number of supplier incidents reported per quarter”). By not providing this, the guideline leaves it to each organization to invent their own metrics, which is inefficient and could result in important aspects being overlooked.

In summary, the lack of explicit KPIs in the guideline was highlighted as a practical shortcoming. Experts felt that including concrete metrics for contract management and supplier monitoring would improve the guideline's usefulness, ensuring that the "monitoring" recommended is not just qualitative or ad-hoc but anchored in continuous, data-driven oversight. This addition would help practitioners know exactly what to monitor in the supplier relationship (e.g., security SLA compliance, frequency of security audits, incident response drill results, etc.), thereby making the guideline's outcomes more measurable and management-friendly.

Resource and capacity constraints for implementation

A broad theme in the expert feedback was concern about the resource intensiveness of executing the full C-SCRM guideline, especially for smaller organizations. While the guideline lays out a comprehensive set of practices, it assumes that organizations can mobilize the necessary people, skills, and budget to perform all these activities (from risk assessments to continuous monitoring and improvement cycles). Multiple experts noted that this may be unrealistic without additional guidance on planning and scaling the effort. In the FACE evaluation scoring, for example, participants flagged "feasibility" issues related to capacity and scalability. One interviewee summarized the challenge starkly: the guideline "adds another level of governance and small organizations... they don't have the people [for it]. So your guideline is great, but who's going to do it?"

This critique underscores that the document does not address how an organization should assess its own capacity or phase the implementation according to available resources. The limitation is twofold: first, the guideline could still overwhelm organizations with limited cybersecurity staff (e.g. an SME with one security officer might find it impossible to instantly operate all the recommended processes).

Second, it provides no advice on leveraging tools or external services to ease the burden. Experts mentioned that smaller enterprises will need "smarter solutions" or external support to implement such a broad program, but the guideline doesn't explicitly mention options like outsourcing certain assessments or using automation to handle volume (e.g. scanning supplier questionnaires).

Another participant gave a concrete example of the scalability problem: "reviewing thousands of contracts [and] gathering all the data in a central place... are things that you will probably run into" when implementing the guideline fully. Yet the guideline does not explicitly warn of this workload or suggest how to prioritize or resource it (aside from the earlier-noted lack of backlog strategy).

This absence of capacity planning guidance is a practical limitation, it leaves organizations to discover the resource requirements on their own, which could lead to underestimation and potential failure of the initiative. In an academic sense, the guideline is sound, but from the practitioner's perspective, it might seem daunting and perhaps unsustainable without additional investment. Experts evaluating the guideline for "sustainability" noted generally that the practices are necessary and not inherently overly costly, but the human factor, having enough skilled personnel and time, is the real constraint.

Therefore, a limitation of the current guideline is that it does not provide a roadmap for scaling according to organizational size or maturity. It treats all organizations as if they can do all tasks, which is not true in reality. A more practical approach (as per the interviews) would be tiered recommendations: e.g., what minimal set of practices to start with if resources are very limited, or guidance on obtaining management buy-in for incremental headcount/tools by demonstrating quick wins.

In conclusion, the expert feedback highlights that the guideline's comprehensiveness comes at the cost of implementation burden, and without explicit discussion of resource and capacity planning, some organizations may find it challenging to translate the guideline into action. This is an important limitation, as it speaks to the feasibility of the guideline in diverse real-world contexts.

Supplier cooperation and power imbalance challenges

An additional practical challenge raised by experts – one not directly addressed in the guideline, is the dependence on supplier cooperation when implementing many of the recommended practices. The guideline presupposes that an organization can impose certain requirements on its suppliers (e.g. asking them to fill out security questionnaires, adhere to new contract clauses, or participate in incident response drills).

However, as one seasoned practitioner pointed out, this presumption doesn't always hold, especially when the client is small or the supplier is a dominant player. In such cases, power dynamics can limit how far the guideline's recommendations can be enforced. One expert shared real-world scenarios where "big companies ... just don't want to engage" in the due diligence process, effectively telling the client "you're not a big enough customer of ours to be able to do the diligence... you only pay us €8000 a year... that's too little for us to even consider participating".

This example exposes a limitation of the guideline: it does not equip practitioners with strategies for when a supplier resists or refuses the security measures the organization attempts to implement. In practice, this might mean a crucial cloud or software provider declines to answer a lengthy risk questionnaire or rejects certain contract clauses, leaving the adopting organization in a bind. The guideline currently offers no advice on handling such situations. For instance, how to evaluate alternative assurance (if the supplier won't answer questions, can the customer rely on publicly available info or certifications?), how to negotiate when the supplier has the upper hand, or how to decide when to accept a risk versus when to escalate or even terminate a non-cooperative supplier relationship.

The experts implied that this is a common practical issue, noting that some suppliers, particularly those providing niche or essential services, may not be easily replaceable, and thus clients often lack leverage. Ignoring this reality is a limitation because it may lead guideline followers to design controls that work on paper but falter in execution. For example, a policy to "assess all vendors annually" cannot be fulfilled if a key vendor flat-out refuses to participate, yet the guideline doesn't discuss contingency plans for such cases.

To mitigate this, practitioners would benefit from guidance like focusing on building leverage early (e.g. during procurement), or using industry consortia to exert collective pressure on critical suppliers, or at least documenting residual risks when supplier cooperation is partial. Since the guideline stays silent on this topic, organizations must rely on their own experience or creativity to handle uncooperative suppliers.

In summary, the expert feedback reveals a real-world limitation of the best-practice guideline: it operates under an assumption of willing supplier participation. The lack of explicit recognition of power imbalances and negotiation challenges is a shortcoming, as managing supplier relationships is at the heart of C-SCRM. Practitioners must often navigate situations where ideal best practices meet hard business realities, a nuance that, if incorporated into the guideline (even as cautionary notes or alternative measures), would make it more robust and realistic.

Conclusion

While the limitations outlined above highlight several areas where the guideline could benefit from greater depth and specificity, it is important to recognize the inherent challenge of integrating such detailed improvements into a document designed to be broadly applicable across industries, sectors, and organizational sizes.

Many of the implementation gaps identified, such as those related to business impact analysis, supplier assurance, and resource planning, require contextual tailoring to be meaningful and actionable. Embedding such specificity directly within a general-purpose guideline risks undermining its versatility and accessibility. Therefore, it is recommended that sector-specific bodies, regulatory authorities, or industry associations take this generalized framework as a foundation and expand upon it by developing tailored versions aligned to the particular risk profiles, regulatory contexts, and maturity levels of their constituencies. In doing so, the practical applicability of the guideline can be significantly enhanced without compromising its core design principles.

6.5 Research limitations

The research methods described in Chapter 2 provided valuable insights but also introduced several methodological limitations that warrant reflection.

First, while semi-structured interviews enabled rich, qualitative data collection, they are inherently subject to certain biases. The flexible nature of this format is suitable for exploratory inquiry. However, it can lead to varying depth and breadth of responses [52]. Moreover, semi-structured interviews are susceptible to interviewer bias, where subtle cues or phrasing may influence how participants frame

their responses [39]. Through subjectivity in the interpretation this bias can also perpetuate during the analysis of the interview [39]. In this research, we limit this second form of bias through the use of grounded theory. The open coding used in grounded theory minimized subjectivity and introduces a form of traceability between the interviews and the identified concepts [40].

A related limitation concerns the composition of the interview sample. The study conducted seven interviews. Grounded theory was used to code and analyze interview data, the small sample size limited the depth of theoretical abstraction typically associated with this approach [40]. Although all interviewees had relevant domain expertise, the over-representation of KPMG-affiliated participants may have introduced a contextual bias toward consulting-centric perspectives on supply chain risk management. This limited and somewhat homogeneous sample restricts the generalizability of the results. The gathered insights might reflect the specific context and collective experiences of the participants and might not capture concerns or practices that are common in other industries, regions, or organizational types. Therefore, caution is warranted in assuming that the results of this research are applicable to all settings without further validation.

Additionally, the literature review methodology, although comprehensive, relied on a combination of Google Scholar, Consensus, and Research Rabbit. While these tools enabled broad coverage and intuitive, efficient discovery of sources, their use also introduces limitations in terms of academic rigor and reproducibility of the search. The relevance rankings are influenced by platform-specific algorithms and partially opaque. This makes it difficult to guarantee that the same sources would be retrieved under different conditions or by another researcher, potentially affecting the replicability of the literature selection process. Although we did not identify any structural problems in the reliability of the tooling, more research is needed to explicitly evaluate how tools like Google Scholar, Consensus, and Research Rabbit differ in the quality and comprehensiveness of results, in order to establish more reproducible search protocols for academic studies.

A final consideration is the use of AI tools for writing refinements in this thesis. Several AI tools have been used to assist with structuring the text and refine language through grammar and style suggestions to improve the readability and clarity of the document. The author takes full responsibility for and ownership of the academic content, ideas, arguments, and conclusions presented in this thesis.

Chapter 7

Conclusions

7.1 Answers to the research questions

This section presents a comprehensive summary of the findings in relation to the research questions presented in Section 1.3. Each sub-question is addressed individually, drawing upon the results of the literature review, expert interviews, and the development and evaluation of the best practice implementation guideline. Together, these answers provide a foundation for responding to the overarching research question concerning the alignment of C-SCRM practices with the NIS2 Directive.

SQ1: How are C-SCRM methods represented in academic and industry literature?
The research identified a substantial body of academic literature and industry publications addressing C-SCRM. Academic works focus primarily on conceptual models, risk classifications, and the theoretical framing of challenges and mitigation strategies. These studies emphasize risk identification, governance, and the technical aspects of cyber threats to be paramount for adequate C-SCRM. However, they often lack actionable implementation strategies or guidance. In contrast, industry literature, notably from NIST and ISO, provides structured frameworks and guidelines that outline high-level best practices for C-SCRM. Nevertheless, these resources are frequently fragmented, vary in scope and depth, and assume a baseline level of cybersecurity maturity, which limits their applicability for smaller or less mature organizations.

SQ2: What are the practical limitations of the available C-SCRM methods in literature?
The investigation into existing methods revealed several practical shortcomings that hinder effective C-SCRM. Current frameworks and standards often remain overly high-level and abstract, offering recommendations on what to do but little insight into how to do it. This lack of operational detail means organizations struggle with implementation. Many approaches also presume a high degree of cybersecurity maturity and resources that many organizations (especially SMEs) do not possess.

Additionally, the C-SCRM landscape is fragmented, organizations are forced to reconcile multiple frameworks (ISO, NIST, sector-specific regulations like DORA) to cover all risk areas. This patchwork leads to complexity and inconsistent adoption, as guidance is not easy to follow and thus not adopted at all in practice.

Furthermore, existing methods can lag behind evolving threats and technologies, remaining static while supply chain cyber risks rapidly change.

In sum, the available C-SCRM methods are limited by a lack of actionable guidance, poor scalability to less mature organizations, fragmented coverage, and outdated or overly generic content. These limitations underscore the need for a more accessible, tailored, and up-to-date implementation approach, which this research seeks to provide.

SQ3: How can best practices for C-SCRM be shaped into an implementation guideline?
The best practices were shaped into a structured and actionable implementation guideline by synthesizing data from academic literature, industry standards, and expert interviews. The development process followed a structured pipeline that included:

1. Extracting practical recommendations from NIST IR 8276 and complementing them with ISO, NIST SP 800-161, and DORA RTS documents;
2. Organizing these recommendations into logically grouped and sequential best practices;
3. Refining the draft guideline based on expert input and feedback. The result is a step-by-step framework organized into four thematic sections: Governance, Strategies and procedures, Monitoring and assessment methods, and Structured risk management.

Each best practice includes contextual information, conditions for success, and guidance on implementation, making the guideline accessible, replicable, and tailored to various organizational contexts.

SQ4: How does our proposed implementation guideline relate to NIS2 article 21.2.d?
Our best practice implementation guideline was benchmarked against the C-SCRM requirements under NIS2, particularly Article 21.2.d and its implicit extensions. The analysis found a strong alignment between the guideline and the NIS2 directive. The guideline covers all ten identified NIS2 obligations relevant to C-SCRM, including comprehensive risk assessment, supply chain security policies, incident handling, continuous monitoring, documentation, contractual requirements, executive responsibility, training, collaboration, and fourth-party risk.

To maximize compliance and traceability, implementers are advised to explicitly map the C-SCRMpolicy developed through the guideline to specific NIS2 requirements. This mapping helps ensure that both explicit and implicit obligations of NIS2 are addressed and that no essential aspect of compliance is overlooked.

The guideline not only supports compliance with NIS2 but also extends its utility by offering granular implementation advice. This ensures that organizations, regardless of size or maturity, can operationalize regulatory requirements effectively. Therefore, it serves both as a compliance support tool and a practical enhancement to supply chain cybersecurity posture.

Main research question: How to confront the challenges in Cyber Supply Chain Risk Management in accordance with NIS2 article 21.2.d?
This research demonstrates that the challenges in C-SCRM can be effectively confronted by developing an integrated best-practice guideline aligned with NIS2. In answer to the main question, the study's approach is to bridge the gap between high-level frameworks and real-world implementation. By consolidating insights from literature and industry and refining them with expert feedback, we produced a practical C-SCRM implementation guideline tailored to address the noted shortcomings of existing methods. The guideline directly tackles the identified challenges, it provides actionable steps (addressing the lack of operational detail), emphasizes scalability for smaller organizations, and unifies fragmented best practices into one coherent program. Critically, it is built in accordance with NIS2 Article 21.2(d).

In summary, confronting C-SCRM challenges per NIS2 is achieved through a best-practice implementation framework that aligns with regulatory requirements while remaining practical for organizations to adopt. This research's outcome, the guideline, serves as a blueprint for organizations to enhance their cyber supply chain resilience in a structured way. By following this guideline, even resource-constrained enterprises can systematically improve their supply chain security posture and attain compliance with NIS2. In doing so, the thesis effectively lowers the barriers to C-SCRM, providing a clear path forward for practitioners to manage cyber supply chain risks in line with evolving regulatory and threat landscapes.

7.2 Contributions

This thesis makes both academic and practical contributions to the field of Cyber Supply Chain Risk Management. The contributions are summarized below.

7.2.1 Academic contributions

This research makes a significant academic contribution by synthesizing and unifying previously fragmented knowledge from both scholarly literature and industry frameworks into an integrated Cyber Supply Chain Risk Management framework. Prior studies in C-SCRM have largely been conceptual or high-level, offering insight into risks and broad controls but lacking detailed implementation guidance.

By bridging academic findings with practical standards (e.g., NIST guidelines and ISO norms), the thesis fills this gap and presents a cohesive best practice model that translates theory into actionable steps. This integrated framework advances the literature by providing implementation-level detail that was previously missing, thereby extending academic understanding of how to operationalize C-SCRM. In sum, the thesis offers a novel scholarly perspective: a design artifact that consolidates disparate insights into one structured approach, laying groundwork for future research to build upon a more holistic C-SCRM implementation paradigm.

7.2.2 Practical contributions

From a practical standpoint, the thesis delivers a tangible best-practice implementation guideline that lowers the barrier to adopting C-SCRM, particularly for small and medium-sized enterprises and organizations with limited cybersecurity maturity.

Unlike generic frameworks, the guideline is clear, accessible, and highly usable, qualities that were validated through expert interviews to ensure real-world relevance. The guideline provides step-by-step recommendations, concrete examples, and contextual guidance, making it easier for practitioners to understand how to implement effective supply chain risk controls.

This user-friendly approach directly addresses common obstacles in the field (such as complexity and resource constraints) by packaging C-SCRM best practices into an actionable form. The result is a practical tool that organizations can readily adopt as a "blueprint" for improving their cyber supply chain resilience, thereby empowering practitioners to proactively manage risks with clarity and confidence.

7.3 Future work

While this research presents a robust and practical implementation guideline for Cyber Supply Chain Risk Management, there are several opportunities for further refinement and validation.

First, future research should address the limitation of partial social validation. Although this study included expert interviews, a broader and more diverse stakeholder base is needed to fully evaluate the social validity of the proposed guideline. As noted by Peters and Heron [60], social validation involves confirming the relevance, acceptability, and perceived effectiveness of best practices from the perspective of the target user group. Future studies should expand the validation effort to include Small and Medium Enterprises (SMEs), public sector organizations, and representatives from various industries to ensure that the implementation guideline meets the needs of a wide range of users.

Second, the findings and structure of this research can serve as the foundational stage of a more extensive DSRM process [59]. Using a Research by Design approach, scholars can iteratively refine and enhance the guideline through real-world applications. This iterative process allows for continued user feedback, improved design artifacts, and deeper integration into organizational practices. In this sense, the current guideline acts as an initial artifact that can be tested, evolved, and formally evaluated within the broader DSRM lifecycle, as outlined by Peffers et al. [59].

Third, empirical testing of the implementation guideline is essential to assess its effectiveness in practice. Ghadge et al. [36] emphasize the need for empirical validation of C-SCRM frameworks, especially in operational contexts. Future studies could implement the guideline within various organizational settings to observe its real-world performance, track improvements in cybersecurity posture, and identify implementation barriers or enablers. Comparative studies could also assess the effectiveness of the guideline against existing methods in achieving NIS2 compliance and reducing supply chain vulnerabilities.

Fourth, future work should consider industry-specific adaptations of the C-SCRM guideline. One limitation noted in our study is the guideline's generalized, one-size-fits-all nature. Different industries face unique supply chain threats, regulatory requirements, and risk priorities. Therefore, researchers and practitioners could collaborate to develop sector-specific extensions or variants of the guideline. By addressing sector-specific needs, these customized guidelines would enhance the relevance and usability of C-SCRM best practices in those environments.

Ultimately, continuing this line of research will contribute to building a more resilient and inclusive cybersecurity landscape, offering tailored solutions that meet both regulatory expectations and practical organizational needs.

Bibliography

[1] Temitayo Oluwaseun Abrahams, Oluwatoyin Ajoke Farayola, Simon Kaggwa, Prisca Ugomma Uwaoma, Azeez Olanipekun Hassan, and Samuel Onimisi Dawodu. Reviewing third-party risk management: best practices in accounting and cybersecurity for superannuation organizations. *Finance & Accounting Research Journal*, 6(1):21–39, 2024.

[2] William C Adams. Conducting semi-structured interviews. *Handbook of practical program evaluation*, pages 492–505, 2015.

[3] Olubunmi Adeolu Adenekan, Chinedu Ezeigweneme, and Excel Great Chukwurah. Strategies for protecting IT supply chains against cybersecurity threats. *International Journal of Management & Entrepreneurship Research*, 6(5):1598–1606, 2024.

[4] AICPA & CIMA. Audit and Assurance: Greater Than SOC 2, 2025. URL `https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2`. Accessed: 2025-06-24.

[5] Aref Alanazi and Zulfiqar Ali Solangi. Cyber supply chain risk management: A conceptual model. In *2023 IEEE 8th International Conference on Engineering Technologies and Applied Sciences (ICETAS)*, pages 1–4. IEEE, 2023.

[6] Saleh Alsulamy, S. Dawood, Mohamed Rafik, and Mohamed Mansour. Industrial sectors' perceptions about the benefits of implementing iso 14001 standard: Manova and discriminant analysis approach. *Sustainability*, 2022.

[7] Anthony Andreoli, Anis Lounis, Mourad Debbabi, and Aiman Hanna. On the prevalence of software supply chain attacks: Empirical study and investigative framework. *Forensic Science International: Digital Investigation*, 44:301508, 2023.

[8] Jefferey Baldwin. *Cyber Supply Chain Risk Management (C-SCRM) across the Defense Industrial Base (DIB): A Cross-Sectional Survey of Nistir 8276 Key Practices*. Capitol Technology University, 2022.

[9] Nadya Bartol. Cyber supply chain security practices DNA–filling in the puzzle using a diverse set of disciplines. *Technovation*, 34(7):354–361, 2014.

[10] Melanie Birks and Jane Mills. Grounded theory: A practical guide, 2022.

[11] Mauricio F Blos, Mohammed Quaddus, HM Wee, and Kenji Watanabe. Supply chain risk management (scrm): a case study on the automotive and electronic industries in brazil. *Supply Chain Management: An International Journal*, 14(4):247–252, 2009.

[12] Jon Boyens, Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi. Key practices in cyber supply chain risk management: Observations from industry. Technical Report NISTIR 8276, National Institute of Standards and Technology, 2021. URL `https://csrc.nist.gov/pubs/ir/8276/final`.

[13] Jon Boyens, Angela Smith, Nadya Bartol, Kris Winkler, Alex Holbrook, and Matthew Fallon. Cybersecurity supply chain risk management practices for systems and organizations. Technical Report NIST SP 800-161 Rev. 1, National Institute of Standards and Technology, 2022. URL `https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final`.

[14] Jon M. Boyens, Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi. Case studies in cyber supply chain risk management: Summary of findings and recommendations. Technical Report NIST.CSWP.02042020-1, National Institute of Standards and Technology, 2020. URL https://csrc.nist.gov/Pubs/cswp/11/case-studies-in-cscrm-summary-of-findings-and-reco/Final.

[15] Sandor Boyson. Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, 34(7):342–353, 2014.

[16] Stuart Bretschneider, Frederick J Marc-Aurele, and Jiannan Wu. "best practices" research: a methodological guide for the perplexed. *Journal of Public Administration Research and Theory*, 15(2):307–323, 2004.

[17] Kam-Fung Cheung, Michael GH Bell, and Jyotirmoyee Bhattacharjya. Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transportation Research Part E: Logistics and Transportation Review*, 146:102217, 2021.

[18] Claudia Colicchia, Alessandro Creazza, and David A Menachof. Managing cyber and information risks in supply chains: insights from an exploratory analysis. *Supply Chain Management: An International Journal*, 24(2):215–240, 2019.

[19] Zachary A Collier and Joseph Sarkis. The zero trust supply chain: Managing supply chain risk in the absence of trust. *International Journal of Production Research*, 59(11):3430–3445, 2021.

[20] The European Commission. Directive (eu) 2022/2555 of the european parliament and of the council of 14 december 2022 on measures for a high common level of cybersecurity across the union, amending regulation (eu) no 910/2014 and directive (eu) 2018/1972, and repealing directive (eu) 2016/1148 (nis 2 directive), 2022. URL https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies. Accessed: (8-Jan.-2025).

[21] The European Commission. "cybersecurity policies", shaping europes digital future, 2023. URL https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies. Accessed: (8-Jan.-2025).

[22] Consensus. Consensus: Ai-powered academic search engine. https://consensus.app/, 2025.

[23] Alessandro Creazza, Claudia Colicchia, Salvatore Spiezia, and Fabrizio Dallari. Who cares? supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. *Supply Chain Management: An International Journal*, 27(1):30–53, 2022.

[24] John W Creswell and Cheryl N Poth. *Qualitative inquiry and research design: Choosing among five approaches*. Sage publications, 2016.

[25] Shannon Eggers. A novel approach for analyzing the nuclear supply chain cyber-attack surface. *Nuclear Engineering and Technology*, 53(3):879–887, 2021.

[26] Daniel Alberto Sepúlveda Estay and Omera Khan. Control structures in supply chains as a way to manage unpredictable cyber-risks. In *5th World Production and Operations Management Conference*, 2016.

[27] European Supervisory Authorities (EBA, EIOPA, and ESMA). Final report on draft regulatory technical standards to specify the policy on ict services supporting critical or important functions. Technical Report JC 2023 84, Joint Committee of the European Supervisory Authorities, January 2024.

[28] European Supervisory Authorities (EBA, EIOPA, and ESMA). Final report on draft regulatory technical standards on ict risk management framework and on simplified ict risk management framework. Technical Report JC 2023 86, Joint Committee of the European Supervisory Authorities, January 2024.

[29] Joseph Farrell and Garth Saloner. Standardization, compatibility, and innovation. *The RAND Journal of Economics*, 16:70–83, 1985.

[30] Flourish. Flourish: Interactive data visualization. https://flourish.studio/, 2025.

[31] World Economic Forum. Global cybersecurity outlook 2024, 2024. URL https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf.

[32] World Economic Forum. Global cybersecurity outlook 2025, 2025. URL https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf.

[33] Anna R Gagliardi and Melissa C Brouwers. Integrating guideline development and implementation: analysis of guideline development manual instructions for generating implementation advice. *Implementation science*, 7:1–9, 2012.

[34] Anisha Banu Dawood Gani, Yudi Fernando, Shulin Lan, Ming K Lim, and Ming-Lang Tseng. Interplay between cyber supply chain risk management practices and cyber security performance. *Industrial Management & Data Systems*, 123(3):843–861, 2022.

[35] Gartner. Gartner identifies three factors influencing growth in security spending, 2022. URL https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i.

[36] Abhijeet Ghadge, Maximilian Weiß, Nigel D Caldwell, and Richard Wilding. Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal*, 25(2):223–240, 2019.

[37] Nourhan Halawi Ghoson, Vincent Meyrueis, Khaled Benfriha, Thomas Guiltat, and Stéphane Loubere. A review on the static and dynamic risk assessment methods for OT cybersecurity in industry 4.0. *Computers & Security*, page 104295, 2024.

[38] Lynda Gratton and Sumantra Ghoshal. Beyond best practice. *MIT Sloan Management Review*, 46 (3):49, 2005.

[39] Dale T. Griffee. Research tips: Interview data collection. *Journal of Developmental Education*, 28: 36–37, 2005.

[40] Grounded Theory Online. What is grounded theory?, 2025. Available: https://www.groundedtheoryonline.com/what-is-grounded-theory/, [Accessed: 28-Jan.-2025].

[41] Badis Hammi, Sherali Zeadally, and Jamel Nebhen. Security threats, countermeasures, and challenges of digital supply chains. *ACM Computing Surveys*, 55(14s):1–40, 2023.

[42] Anders Hansen Henten, Iwona Windekilde, and Morten Falch. Cybersecurity institution in the EU and the US, 2024.

[43] William Ho, Tian Zheng, Hakan Yildiz, and Srinivas Talluri. Supply chain risk management: a literature review. *International journal of production research*, 53(16):5031–5069, 2015.

[44] IBM. Cybersecurity, 2025. Available: https://www.ibm.com/think/topics/cybersecurity, [Accessed: 15-Jan.-2025].

[45] International Organization for Standardization. Iso/iec 27002:2022: Information security, cybersecurity and privacy protection - information security controls - third edition 2022-02. Standard, International Organization for Standardization, 2022.

[46] Shazia Jamshed. Qualitative research method-interviewing and observation. *Journal of basic and clinical pharmacy*, 5(4):87, 2014.

[47] Amer Jazairy, Mazen Brho, Ila Manuj, and Thomas J Goldsby. Cyber risk management strategies and integration: toward supply chain cyber resilience and robustness. *International Journal of Physical Distribution & Logistics Management*, 54(11):1–29, 2024.

[48] SZ Kamal, SM Al Mubarak, BD Scodova, P Naik, P Flichy, and G Coffin. IT and OT convergence-opportunities and challenges. In *SPE Intelligent Energy International Conference and Exhibition*, pages SPE–181087. SPE, 2016.

[49] Monika Kastner, Onil Bhattacharyya, Leigh Hayden, Julie Makarski, Elizabeth Estey, Lisa Durocher, Ananda Chatterjee, Laure Perrier, Ian D Graham, Sharon E Straus, et al. Guideline uptake is influenced by six implementability domains for creating and communicating guidelines: a realist review. *Journal of clinical epidemiology*, 68(5):498–509, 2015.

[50] Olivier Lavastre, Angappa Gunasekaran, and Alain Spalanzani. Effect of firm characteristics, supplier relationships and techniques used on supply chain risk management (scrm): an empirical investigation on french industrial firms. *International Journal of Production Research*, 52(11):3381–3403, 2014.

[51] Jonathan D Linton, Sandor Boyson, and John Aje. The challenge of cyber supply chain security to research and practice–an introduction, 2014.

[52] R. Longhurst. Interviews: In-depth, semi-structured, 2009.

[53] Kaspar Rosager Ludvigsen, Shishir Nagaraja, and Angela Daly. Preventing or mitigating adversarial supply chain attacks: A legal analysis. In *Proceedings of the 2022 ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses*, pages 25–34, 2022.

[54] Helen Viktoria Lust. Complying with supply chain security requirements under the nis-2 directive balancing the intersection between nis-2 directive and gdpr compliance in supplier monitoring. Master's thesis, University of Oslo, 2023.

[55] Mamad Mohamed. Challenges and benefits of industry 4.0: An overview. *International Journal of Supply and Operations Management*, 5(3):256–265, 2018.

[56] National Institute of Standards and Technology (NIST). Cyber supply chain risk management (c-scrm), 2025. Available: `https://csrc.nist.gov/projects/cyber-supply-chain-risk-management`, [Accessed: 20-Jan.-2025].

[57] National Institute of Standards and Technology. Security and privacy controls for information systems and organizations. Technical Report NIST SP 800-53 Rev. 5, National Institute of Standards and Technology, 2020. URL `https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final`.

[58] Shipra Pandey, Rajesh Kumar Singh, Angappa Gunasekaran, and Anjali Kaushik. Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, 13(1):103–128, 2020.

[59] Ken Peffers, Tuure Tuunanen, Marcus A Rothenberger, and Samir Chatterjee. A design science research methodology for information systems research. *Journal of management information systems*, 24(3):45–77, 2007.

[60] Mary T Peters and Timothy E Heron. When the best is not good enough: An examination of best practice. *The journal of special education*, 26(4):371–385, 1993.

[61] Matteo Podrecca, Giovanna Culot, Guido Nassimbeni, and Marco Sartor. Information security and value creation: The performance implications of iso/iec 27001. *Computers in Industry*, 142:103744, 2022.

[62] Jonathan Pollet and Joe Cummins. All hazards approach for assessing readiness of critical infrastructure. In *2009 IEEE Conference on Technologies for Homeland Security*, pages 366–372. IEEE, 2009.

[63] Kevin Pottie, Olivia Magwood, Prinon Rahman, Thomas Concannon, Pablo Alonso-Coello, Alejandra Jaramillo Garcia, Nancy Santesso, Brett Thombs, Vivian Welch, George A Wells, et al. Grade concept paper 1: Validating the "face" instrument using stakeholder perceptions of feasibility, acceptability, cost, and equity in guideline implement. *Journal of Clinical Epidemiology*, 131:133–140, 2021.

[64] Mehrdokht Pournader, Andrew Kach, and Srinivas Talluri. A review of the existing and emerging topics in the supply chain risk management literature. *Decision sciences*, 51(4):867–919, 2020.

[65] Research Rabbit. Research rabbit: The most powerful discovery app for researchers. `https://www.researchrabbit.ai/`, 2025.

[66] Alberto Redondo, Alberto Torres-Barrán, David Ríos Insua, and Jordi Domingo. Assessing supply chain cyber risks. *arXiv preprint arXiv:1911.11652*, 2019.

[67] Ronald S Ross. Risk management framework for information systems and organizations: A system life cycle approach for security and privacy, 2018.

[68] Jukka Ruohonen. A systematic literature review on the nis2 directive. *arXiv preprint arXiv:2412.08084*, 2024.

[69] P.N. Sindhuja and Anand S Kunnathur. Information security in supply chains: A management control perspective. *Information & Computer Security*, 23(5):476–496, 2015.

[70] Theresa Sobb, Benjamin Turnbull, and Nour Moustafa. Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. *Electronics*, 9(11):1864, 2020.

[71] Anselm Strauss, Juliet Corbin, et al. *Basics of qualitative research*, volume 15. sage Newbury Park, CA, 1990.

[72] Anselm L Strauss. *The discovery of grounded theory: Strategies for qualitative research*. Routledge, 2017.

[73] H. Su, Suvrat S. Dhanorkar, and K. Linderman. A competitive advantage from the implementation timing of iso management standards. *Journal of Operations Management*, 37:31–44, 2015.

[74] Uchenna Joseph Umoga, Enoch Oluwademilade Sodiya, Olukunle Oladipupo Amoo, Akoh Atadoga, et al. A critical review of emerging cybersecurity threats in financial technologies. *International Journal of Science and Research Archive*, 11(1):1810–1817, 2024.

[75] Alwin van Welie. Legislation within cybersecurity: preparing for nis2–a detailed framework in the, 2024.

[76] Niels Vandezande. Cybersecurity in the eu: How the nis2-directive stacks up against its predecessor. *Computer Law & Security Review*, 52:105890, 2024.

[77] Luit Verschuur. Towards a cybersecurity assessment framework for iot-based environments, 2022.

[78] Gary Whited, Awad Hanna, et al. Best practices from wisdot mega and arra projects: best practice catalog. Technical report, University of Wisconsin–Madison. Construction and Materials Support Center, 2012.

[79] Marjorie Windelberg. Objectives for managing cyber supply chain risk. *International Journal of Critical Infrastructure Protection*, 12:4–11, 2016.

[80] Jiannan Wu, Yao Liu, and Stuart Bretschneider. Best practice is not just "best": An empirical study based on judges' perceptions. *Urban Governance*, 3(2):130–137, 2023.

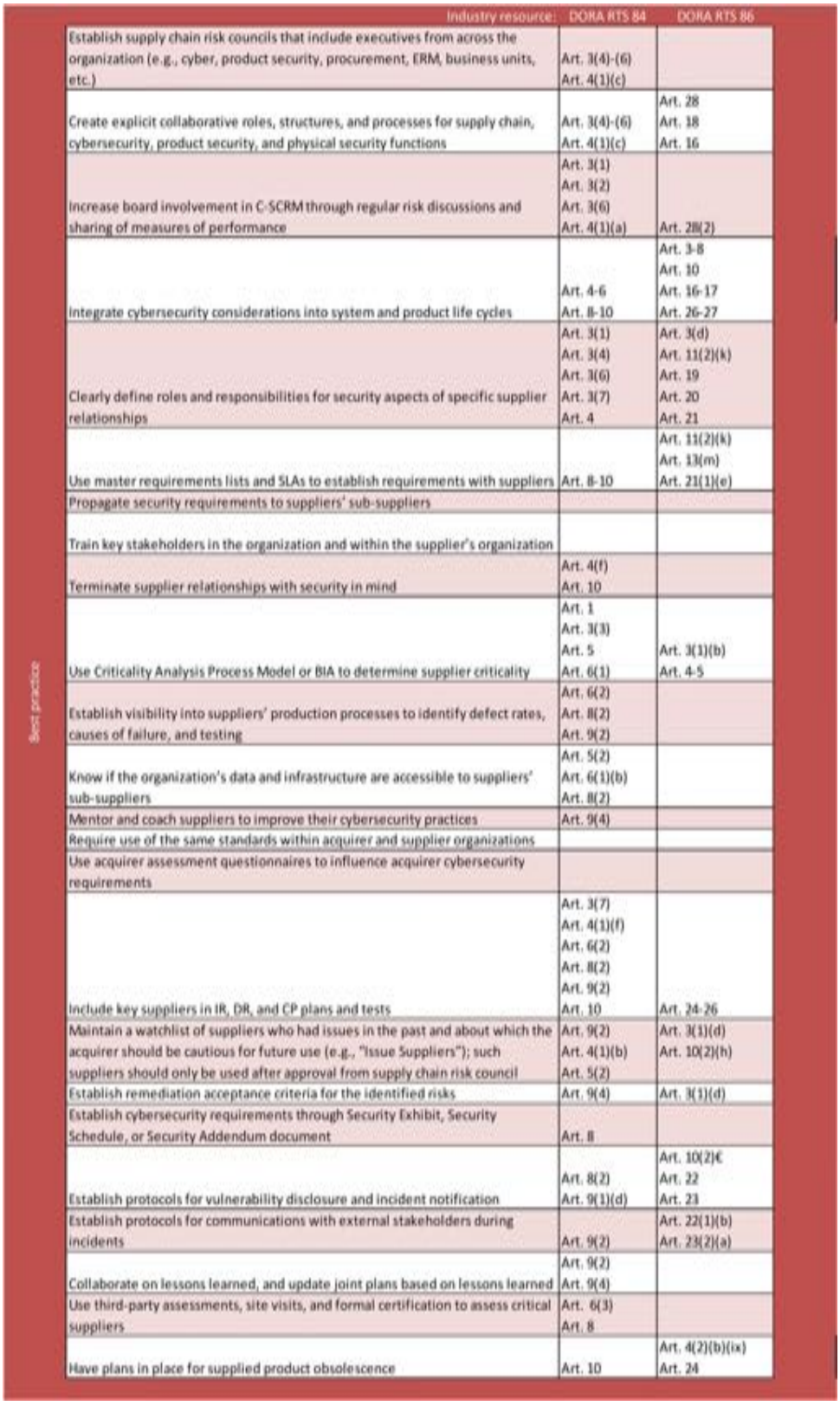
[81] Yun Xu, W. Boh, Chuan Luo, and Haichao Zheng. Leveraging industry standards to improve the environmental sustainability of a supply chain. *Electron. Commer. Res. Appl.*, 27:90–105, 2018.

[82] Kaiyue Zheng and Laura A Albert. A robust approach for mitigating risks in cyber supply chains. *Risk Analysis*, 39(9):2076–2092, 2019.

Appendix A

NIST IR 8276 and DORA RTS mapping

Figure A.1 present our mapping between the NIST IR 8276 [12] key recommendations to specific articles within both the DORA RTS 84 on ICT Risk Management Framework and the DORA RTS 86 on ICT services supporting critical or important functions, showing which specific articles advice or provides guidance on implementation of each recommendation. This mapping functions as substantiation for our original expansion of the NIST IR 8276 mapping to industry resources.



Industry resource:	DORA RTS 84	DORA RTS 86
Establish supply chain risk councils that include executives from across the organization (e.g., cyber, product security, procurement, ERM, business units, etc.)	Art. 3(4)-(6) Art. 4(1)(c)	
Create explicit collaborative roles, structures, and processes for supply chain, cybersecurity, product security, and physical security functions	Art. 3(4)-(6) Art. 4(1)(c)	Art. 28 Art. 18 Art. 16
Increase board involvement in C-SCRM through regular risk discussions and sharing of measures of performance	Art. 3(1) Art. 3(2) Art. 3(6) Art. 4(1)(a)	Art. 28(2)
Integrate cybersecurity considerations into system and product life cycles	Art. 4-6 Art. 8-10	Art. 3-8 Art. 10 Art. 16-17 Art. 26-27
Clearly define roles and responsibilities for security aspects of specific supplier relationships	Art. 3(1) Art. 3(4) Art. 3(6) Art. 3(7) Art. 4	Art. 3(d) Art. 11(2)(k) Art. 19 Art. 20 Art. 21
Use master requirements lists and SLAs to establish requirements with suppliers	Art. 8-10	Art. 11(2)(k) Art. 13(m) Art. 21(1)(e)
Propagate security requirements to suppliers' sub-suppliers		
Train key stakeholders in the organization and within the supplier's organization		
Terminate supplier relationships with security in mind	Art. 4(f) Art. 10	
Use Criticality Analysis Process Model or BIA to determine supplier criticality	Art. 1 Art. 3(3) Art. 5 Art. 6(1)	Art. 3(1)(b) Art. 4-5
Establish visibility into suppliers' production processes to identify defect rates, causes of failure, and testing	Art. 6(2) Art. 8(2) Art. 9(2)	
Know if the organization's data and infrastructure are accessible to suppliers' sub-suppliers	Art. 5(2) Art. 6(1)(b) Art. 8(2)	
Mentor and coach suppliers to improve their cybersecurity practices	Art. 9(4)	
Require use of the same standards within acquirer and supplier organizations		
Use acquirer assessment questionnaires to influence acquirer cybersecurity requirements		
Include key suppliers in IR, DR, and CP plans and tests	Art. 3(7) Art. 4(1)(f) Art. 6(2) Art. 8(2) Art. 9(2) Art. 10	Art. 24-26
Maintain a watchlist of suppliers who had issues in the past and about which the acquirer should be cautious for future use (e.g., "Issue Suppliers"); such suppliers should only be used after approval from supply chain risk council	Art. 9(2) Art. 4(1)(b) Art. 5(2)	Art. 3(1)(d) Art. 10(2)(h)
Establish remediation acceptance criteria for the identified risks	Art. 9(4)	Art. 3(1)(d)
Establish cybersecurity requirements through Security Exhibit, Security Schedule, or Security Addendum document	Art. 8	
Establish protocols for vulnerability disclosure and incident notification	Art. 8(2) Art. 9(1)(d)	Art. 10(2)€ Art. 22 Art. 23
Establish protocols for communications with external stakeholders during incidents	Art. 9(2)	Art. 22(1)(b) Art. 23(2)(a)
Collaborate on lessons learned, and update joint plans based on lessons learned	Art. 9(2) Art. 9(4)	
Use third-party assessments, site visits, and formal certification to assess critical suppliers	Art. 6(3) Art. 8	
Have plans in place for supplied product obsolescence	Art. 10	Art. 4(2)(b)(ix) Art. 24

Figure A.1: Mapping of key recommendations from NIST IR 8276 [12] to the DORA RTS 84 & 86 articles.

Appendix B

Semi-structured interview guide

1. Ask for consent to make audio recording of the interview.
   - Explain the purpose of the audio recording.
   - Explain processing of audio recording (transcription, anonymization).
   - Discuss the retention period of the recording.
   - Explain that the interviewee can stop the interview at any time, withdraw consent to participate in the research, and coincidentally request deletion of the recording and exclusion of the study.
   - Ask: “Do you understand these conditions and give me consent to record this interview?"
2. Discuss the purpose and scope of the research.
3. Discuss structure of the interview.
   - Personal information of the interviewee.
   - Personal experience with C-SCRM.
   - Verification of information gathered up till this point.
   - Exploration of perception on the developed best practices implementation guideline.
4. Discuss personal profile of interviewee:
   - Could you describe your field of expertise, how long you have been working in this field and provide some details about your educational and professional background?
   - What is your current role, and what are your main activities and responsibilities in this position?
   - In which country do you work, and how does your work environment differ from that in other countries, such as in terms of specialized offices or clients?
5. Discuss personal experience of interviewee with C-SCRM:
   - How would you define Cyber Supply Chain Risk Management (C-SCRM) from your perspective?
   - Do you have any experience with C-SCRM practices? If not, what related experiences do you have that come closest?
     - Have you encountered specific problems or gaps in the process?
     - Did you identify possible improvement opportunities during this experience
6. Gather insight on C-SCRM challenges, risks, sources and measures:
   - What are the biggest challenges your organization faces in actively managing cyber risks in the supply chain?

- Which types of cyber risks do you consider most critical when aiming to strengthen supply chain resilience?
- In your experience, what are the most common sources of cyber risk within the supply chain?
- What high-level strategies or measures do you believe are essential when establishing an effective C-SCRM function?

7. Discuss possible gaps in C-SCRM guidance documents.
   - Are you familiar with specific guidelines or frameworks that can be implemented to improve supply chain cybersecurity?
   - Have you used these guidelines or frameworks or worked at organizations were these were prescribed for adoption?
   - Do you find these guidance documents pose a challenge for some organizations to implement correctly? If so, how can these types of guidelines/frameworks be improved to close this gap?
8. Discuss the developed implementation guideline:
   - Gather viewpoints on the 17 best practice titles.
   - Gather viewpoints on the overview demonstrator.
   - Gather viewpoints on specific best practices content based on the interviewees domain of expertise.
9. Gather FACE data, ask to answer: yes/probably no/no/varies/don't know; then, explore answer:
   - Do you consider the lack of actionable guidance that lowers the expertise for establishing and operating a C-SCRM capability a priority issue within the field?
   - Would the implementation of the practices and recommendations outlined in the C-SCRM guideline be sustainable? Would there be important barriers that are likely to limit the feasibility of implementing them?
   - Do you feel the guideline would be acceptable to stakeholders involved in implementation?
   - Do you feel that implementation of the guideline would be costly to stakeholders?
   - Do you feel that implementation of the guideline would positively impact the inequity between organizations with differing resources and levels of cybersecurity maturity (e.g., SMEs vs. large enterprises)?
   - Based on your current understanding, would you intend to adopt or integrate the recommendations in this C-SCRM guideline into existing risk management practices?
10. Close of interview:
    - Are there any other topics you find relevant to discuss or mention in the domain of C-SCRM?
    - Are you available for follow-up questions?

Appendix C

Academic literature review data

Figure C presents the raw data collected from all academic articles included in our literature review. The data are compiled in an table displaying the data per article collected in the categories of identified Threats, Sources of threats, Challenges and Measures. This data is compiled into key insights presented in Section 3.2

#	Citation	Title of Papers	Year	Summary	Key take aways	Threats	Sources of Threats	Challenges	Measures	Keywords
1	Colicchia, C., Creazza, A., & Menachof, D. A. (2019). Managing cyber and information risks in supply chains: insights from an exploratory analysis. *Supply Chain Management: An International Journal*, *24*(2), 215-240.	Managing cyber and information risks in supply chains: insights from an exploratory analysis	2019	Analysis and classification of cyber and information risks, sources of risks and initiatives to managing them according to a supply chain perspective, along with an investigation of their adoption across the supply chain	Companies need to move beyond isolated IT solutions and adopt a comprehensive, supply chain-wide approach to manage cyber risks effectively, involving all stakeholders and focusing on both technical and organizational measures.	**Customer Records Compromised**: Highly disruptive and impactful on business, particularly affecting reputation and competitive advantage. **Failure of Companies' IT Network**: Highly disruptive with a high probability of occurrence. **Cyber-Attacks Affecting Downstream Supply Chain**: Concerns about the impact on relationships with customers and overall business reputation. **Risks Affecting Suppliers' Records**: Noted risk, though less concerning to some companies. **General Cyber and Information Risks**: Varying perceptions among companies, with some having higher awareness due to recent incidents. **Data Breach/Disclosure**: Unauthorized access and exposure of sensitive information. **Theft of Intellectual Property**: Stealing proprietary information for competitive advantage. **IT System Failures**: Crashes and failures of IT infrastructure. **Cyber Attacks**: Malicious attacks from hackers and cyber terrorists. **Social Engineering**: Manipulating employees to divulge confidential information. **Natural Disasters**: Events like power outages and technical problems disrupting operations.	**Employees (Current and Former)**: Both malicious and non-intentional actions by employees are significant sources of cyber and information risks. **Internal Sources within the Focal Company**: Risks that originate internally but can spread across the entire supply chain. **Upstream Supply Chain Stages**: Suppliers or contractors beyond Tier 1 are critical sources of risk due to lack of visibility and control. **Critical Infrastructural Nodes**: Ports and organizations handling data at these nodes, such as port operators, are sources of cyber risk. **Distant Supply Chain Players**: Subcontractors and other players in the distant stages of the supply chain, where lack of visibility and control is a concern. **Customers**: Risks from data sharing and transmission with customers. **Competitors**: Industrial espionage and data misappropriation. **Foreign Nation States:** Espionage and cyber attacks from foreign entities. **Hackers/Hacktivists**: Malicious cyber attacks from external actors. **Natural Disasters**: Non-intentional disruptions like power outages and technical failures.	**Lack of Visibility:** Difficulty in seeing beyond Tier 1 suppliers. **Isolation in Decision-Making**: Decisions are often made in isolation without involving supply chain partners. **Complexity of Supply Chains**: Managing risks in complex, multi-tiered supply chains. **Employee Awareness**: Ensuring employees are aware of cyber risks and their impact. **Balancing Security and Performance**: Trade-offs between network security and operational performance. **Resource Allocation**: Difficulty in justifying investments in CSCRM initiatives.	**Organizational Initiatives** **Information Security Strategy Alignment**: Aligning the information security strategy with the overarching business strategy and specific needs. **Standards and Protocols**: Adoption of standards like ISO27000 and NIST SP 800-161 to improve strategic alignment and provide regulatory guidelines. **Chief Information Security Officer (CISO)**: Establishing a CISO position to oversee information security. **Personnel Background Checks**: Conducting background checks on personnel to ensure security. **Cyber Insurance**: Adoption of cyber insurance products to tackle cyber threats, though their adoption is still in its infancy. **Training and Internal Awareness** **Cyber Hygiene Training**: Educating employees on good network usage practices. **Security Awareness Programs**: Programs to up-skill human capital to enhance resilience and prevent, detect, and respond to internal threats. **Employee Awareness**: Strengthening staff awareness to help directors and top management in driving security investment and supplier selection. **Intellectual Property Protection**: Procedures for protecting intellectual property, including safe and controlled sharing of data across multiple tiers of the supply chain. **Compliance and External Awareness** **Privacy and Security Policies Compliance**: Requiring customers and suppliers/contractors to comply with privacy and security policies. **Supply Chain Partner Security Audits**: Conducting security audits and qualification/operational checks on supply chain partners. **Collaborative Agreements**: Establishing collaborative agreements with supply chain partners on security to create end-to-end IT integration. **Supply Chain Coordination Mechanisms**: Achieving alignment, synchronization, and shared knowledge among supply chain partners. **Event Management** **Business Continuity and Disaster Recovery Plans**: Implementing plans to ensure continuity and recovery from disruptions. **Incident Management Processes**: Processes to manage and respond to cyber and information risk events. **Communication Procedures**: Establishing communication procedures with involved supply chain partners to improve response and recovery effectiveness. **Information Systems Continuity Management**: Approaches to identify dependencies between internal and external systems and supply chain players. **Data Management** **Accurate Record of Personnel Handling Data**: Maintaining accurate records of employees accessing and handling data. **Secure Data Access and Control Measures**: Implementing measures to secure data access and control. **Privileged User Access**: Allocating access permissions and privileges to different categories of users. **Identification of Sensitive Assets**: Programs to identify sensitive assets and prevent leakage of confidential information. **IT Security Tools** **Encryption of Email Messages**: Encrypting email messages to protect data. **Intrusion Prevention Systems (IPS)**: Using IPS to detect and prevent unauthorized access. **Data Loss Prevention Tools**: Tools to prevent data loss. **Mobile Security Strategy and Device Management**: Strategies to secure mobile devices. **Geo-location and Geo-fencing Controls**: Using firewalls and virtual private networks (VPN) for geo-location and geo-fencing. **Data and URL Filtering**: Implementing antivirus and antispam tools for data and URL filtering. **IT Operational Resilience** **Internal Recovery Plan Processes**: Processes to ensure internal recovery from IT failures. **Collaborative Recovery Plan Processes**: Collaborative recovery plans involving supply chain partners. **Multiple Data Backup**: Ensuring multiple backups of data. **Geographical Distributed Datacentres**: Using geographically distributed datacentres for resilience. **Virtual Networks/IT Infrastructures**: Implementing virtual networks and IT infrastructures. **Cloud Systems Orchestrators**: Using cloud systems orchestrators to isolate networks during cyber-attacks while maintaining operations. **Uninterruptible Power Supplies/Power Banks**: Ensuring continuity of operations with uninterruptible power supplies and power banks.	Supply chain risk management; Cyber risk; Information risk; Cyber security; Supply chain management; Supply chain resilience;
2	Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2019). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal*, *25*(2), 223-240.	Managing cyber risk in supply chains: A review and research agenda	2019	Systematic literature review on managing cyber risks in supply chains and develops a conceptual model for supply chain cyber security systems and an agenda for future studies.	Holistic guide for practitioners in understanding cyber-physical systems. The cyber risk challenges and the mitigation strategies identified support supply chain managers in making informed decisions.	**Physical threats** Disruption to the functioning or deliberate damaging or theft of physical infrastructure components. **Breakdown** Not deliberate; Systems or resources breaking down, such as outdated firewalls or landing pages. **Indirect attacks** Denial of service or password sniffing. **Direct attacks** Virus attack/hacking attacks impacting the operations, counterfeit products, and spoofing attacks. **Insider threats** Carelessness, lack of awareness, intentions, or indebted accidents by employees.	**Technical Points of Penetration** **IT-Related Assets**: All IT-related assets, including systems, software, personnel, and equipment, are prone to cyber risks. **Legacy Systems:** Outdated and poorly maintained systems are particularly vulnerable to attacks. **Outsourcing Servers**: While outsourcing servers can reduce upfront costs, it may increase long-term indirect costs due to loss of control over security. **Human Points of Penetration** **Human Involvement:** Cyber security is not just about technical solutions; human involvement is crucial. **Susceptible Stakeholders:** Companies are only as secure as their most vulnerable stakeholders. **Internal Human Errors:** These errors can have severe consequences and are challenging to identify. **Exploitation by Cyber Aggressors:** Future cyber risks are expected to exploit human vulnerabilities, especially when employees interact across organizational boundaries. **Physical Points of Penetration** **Physical Objects**: Buildings, machines, and other physical surroundings can be points of penetration for cyber risks. **Obsolete Firewalls:** Inadequate control mechanisms can allow attackers to gain remote access to systems. **Vulnerability to Disasters:** Physical infrastructures are also vulnerable to natural disasters or physical attacks that impact cyber systems.	**Inter-organizational Collaboration:** Lack of accepted standards and guidelines hinders robust cyber defenses, requiring transparent and trust-based relationships among supply chain partners. **Employee Knowledge**: The challenge of hiring and training cybersecurity-skilled employees to proactively manage and pre-empt cyber risks. **Continuous Commitment:** The need for ongoing commitment and shared responsibility across departments to manage evolving cyber risks. **Governmental Involvement:** Governments need to sponsor and guide cyber security projects, creating forums for better communication and strategy planning.	**Pre-attack phase** Access control Accreditation against security standards Certified hard- and software Cross-functional communication Formal agreements between SC partners Information sharing Internalisation of operations More sophisticated and diverse applications Network audit Risk awareness initiatives Risk classification Risk identification software Standard guidelines for SC collaboration Supplier audit Training Vulnerability checks "Zero-trust" policy **Trans-attack phase** Data consistency checks Task force **Post-attack phase** Forensics Incident documentation Insurances Recovery and backup procedures	Risk management; Cybersecurity, Text mining; Systematic literature review; Supply chain disruptions; Supply chain risk management; Supply risk; Supply chain resilience; Cyber-attacks; Cyber risks; Cyber resilience;
3	Zheng, K., & Albert, L. A. (2019). A robust approach for mitigating risks in cyber supply chains. *Risk Analysis*, *39*(9), 2076-2092.	A robust approach for mitigating risks in cyber supply chains	2019	Proposes three alternative models that consider different robustness methods that hedge against worst-case risks	Offers a quantitative way of selecting mitigation measures	**Counterfeit Materials**: Use of fake or substandard materials in the supply chain. **Malicious Software**: Introduction of malware through various points in the supply chain. **Unqualified Vendors:** Engagement with vendors who do not meet security standards. **Poorly Trained Employees**: Employees lacking proper training in cybersecurity practices.	**Third-Party Suppliers**: Vulnerabilities originating from third-party suppliers and vendors. **Global Supply Chains**: Risks introduced by the globalization and complexity of supply chains. **Handling and Distribution**: Weak links in the handling and distribution processes. **Manufacturing and Processing**: Vulnerabilities in the manufacturing and processing stages of the supply chain.	**Uncertain Mitigation Effectiveness**: Difficulty in predicting the effectiveness of security mitigations due to evolving cyber threats and limited knowledge. **Budget Constraints**: Limited financial resources for selecting and deploying security mitigations. **Complex Attack Paths**: Multiple vulnerabilities and attack paths that need to be covered, making it challenging to prioritize mitigations. **Worst-Case Scenarios**: Need to prepare for worst-case scenarios which may require different strategies than average-case scenarios. **Adaptive Adversaries**: Adversaries that adapt their strategies, making it difficult to predict and counteract their actions.	**Quantitative Measure Selection**: use quantitative methods to elimnte uncertainties in the process of selecting mitigation approaches.	Cybersecurity; infrastructure risk mitigation; robust optimization;
4	Alanazi, A., & Solangi, Z. A. (2023, October). Cyber Supply Chain Risk Management: A Conceptual Model. In *2023 IEEE 8th International Conference on Engineering Technologies and Applied Sciences (ICETAS)* (pp. 1-4). IEEE.	Cyber Supply Chain Risk Management: A Conceptual Model	2023	Creates a model to help managers better understand and implement the CSCRM process and increase supply chain resilience to cyber threats	Cyber Supply Chain Risk Management requires a holistic approach that integrates technical, human and operational factors, continuous collaboration, and alignment with business goals to enhance cyber resilience.	**Cyber-Attacks:** Threats from malicious cyber activities targeting supply chain systems and data. **Data Breaches:** Unauthorized access to sensitive information within the supply chain. **Phishing Attacks:** Deceptive attempts to obtain sensitive information through fraudulent communications. **Insider Threats:** Risks posed by employees or other insiders who may intentionally or unintentionally compromise security. **Supply Chain Disruptions:** Interruptions in the supply chain caused by cyber incidents affecting suppliers or logistics. **Intellectual Property Theft:** Unauthorized access and theft of proprietary information and trade secrets. **System Vulnerabilities:** Exploitation of weaknesses in outdated or poorly maintained IT systems.	**External Cyber-Attackers:** Malicious entities outside the organization targeting supply chain systems. **Internal Insiders:** Employees or insiders who may intentionally or unintentionally compromise security. **Third-Party Vendors:** Suppliers and service providers that may introduce vulnerabilities into the supply chain. **Outdated Systems:** Legacy IT systems that are poorly maintained and susceptible to exploitation. **Human Errors:** Mistakes made by employees, such as falling for phishing attacks or mishandling sensitive information. **Physical Infrastructure:** Vulnerabilities in physical assets like buildings and machinery that can be exploited for cyber-attacks. **Geopolitical Factors:** Political and regulatory environments that can impact the security of supply chains.	**Complexity of Supply Chains:** Managing cyber risks is challenging due to the horizontal, vertical, and spatial complexity of supply chains. **Lack of Industry-Specific Models**: Existing CSCRM models often fail to accommodate the specific needs of different industries. **Integration with Other Risk Management Systems:** CSCRM models are often siloed and not integrated with other risk management systems, leading to gaps in coverage. **Alignment with Business Goals:** CSCRM models are frequently not aligned with business goals, reducing their effectiveness. **Human Factors:** Cyber risks can arise from human errors, such as phishing attacks or insider threats, which are often overlooked in technical-focused models.	**Risk Identification:** Identifying potential cyber risks within the supply chain. **Risk Assessment:** Evaluating the likelihood and impact of identified risks. **Risk Mitigation:** Implementing strategies to reduce or eliminate risks. **Continuous Monitoring:** Ongoing surveillance of the supply chain to detect and respond to cyber threats. **Employee Training:** Educating employees on cyber security best practices and threat awareness. **Collaboration with Partners:** Working with supply chain partners to enhance overall security. **Use of Technology:** Employing advanced technologies such as firewalls, intrusion detection systems, and encryption to protect data and systems.	Cybersecurity; Supply Chain; Risk management;
5	Redondo, A., Torres-Barrán, A., Insua, D. R., & Domingo, J. (2019). Assessing Supply Chain Cyber Risks. *arXiv preprint arXiv:1911.11652*.	Assessing Supply Chain Cyber Risks	2019	A general approach to support supply chain cyber risk management taking into account various techniques of attacking an organisation and its suppliers, as well as the impacts of such attacks	Use quantified indices within the adopted C-SCRM framework.	**Direct Attacks**: Cyber attacks targeting the company directly. **Indirect Attacks**: Attacks on suppliers that transfer to the company. **Service Unavailability**: Disruption of services due to cyber attacks. **Reputational Damage**: Loss of reputation leading to customer loss.	**Botnets**: Networks of infected devices used to launch attacks. **Stolen Login Information**: Unauthorized access using compromised credentials. **Malware**: Malicious software causing various levels of harm. **Hacktivist Activities**: Negative mentions and activities in hacktivist blogs.	**Data Scarcity**: Lack of sufficient data on cyber attacks due to reputational concerns. **Complexity of Attack Vectors**: Multiple types of attacks and their varying impacts. **Interconnectivity**: Increased risk due to interconnected supply chains. **Expert Judgment Reliance**: Dependence on expert judgment for parameter estimation. **Dynamic Risk Environment**: Constantly evolving cyber threats and security postures.	**Risk Monitoring**: Using forecasting models to predict and monitor risks. **Supplier Management**: Ranking suppliers based on induced risks and impacts. **Service Level Agreements** (SLAs): Use quantified indices when negotiating SLAs and other requirements to manage supplier risks.	Cybersecurity; Risk Analysis; Supply Chain Risks; Expert Judgment;
6	Windelberg, M. (2016). Objectives for managing cyber supply chain risk. *International Journal of Critical Infrastructure Protection*, *12*, 4-11.	Objectives for managing cyber supply chain risk	2016	Proposes a model that focusses on the objectives of security, reliability, safety, quality and trustworthiness	**Tampering:** Unauthorized alterations to hardware or software components. **Counterfeits:** Use of fake or substandard parts within the supply chain. **Poor Quality:** Inadequate quality control leading to vulnerabilities. **Natural Disasters:** Disruptions caused by environmental events. **Human Error:** Mistakes made by individuals that compromise security. **Insider Threats:** Malicious actions by trusted individuals within the organization.	**Adversarial Actions:** Intentional threats such as tampering and counterfeits. **Non-Adversarial Factors:** Unintentional issues like poor quality and natural disasters. **Human Error:** Mistakes made by individuals that can compromise security. **Insider Threats:** Malicious actions by trusted individuals within the organization.	**Comprehensive Risk Coverage:** Ensuring all potential risks are identified and managed effectively. **Technological Vulnerabilities:** Addressing weaknesses in hardware and software components. **Human Factors:** Mitigating risks associated with human error and insider threats. **Stakeholder Collaboration:** Facilitating effective communication and cooperation among all parties involved. **Regulatory Compliance:** Adhering to various legal and regulatory requirements. **Supply Chain Complexity:** Managing the intricate and interconnected nature of modern supply chains.	**Risk Assessment**: Regularly evaluating potential risks within the supply chain to identify and manage vulnerabilities. **Supplier Vetting:** Thoroughly assessing and selecting suppliers based on their security practices to ensure a secure supply chain. **Security Standards**: Implementing and adhering to industry security standards and best practices to maintain a high level of security. **Continuous Monitoring:** Ongoing surveillance of the supply chain to detect and respond to threats in real-time. Incident Response Plans: Developing and maintaining plans to address security incidents promptly and effectively. **Training and Awareness:** Educating employees and stakeholders about security risks and best practices to foster a security-conscious culture. **Security:** Maintaining an authorized state of an element and preventing violations through authorization to interact with components and controlling access. **Reliability:** Ensuring service delivery through redundancy, diversification, independent components, and flexibility to prevent faults and failures. **Safety**: Containing adverse consequences by complying with safety standards (e.g., IEC 61508), designing for degraded mode operations, and using redundancy and containment strategies. **Quality**: Ensuring conformance to specifications and eliminating defects through assurance techniques, including independent validation and verification testing. **Trustworthiness**: Building confidence in performance through adherence to standards, good practices, and exercising due care and due diligence.	Risk management; Information and communications technology; Hardware; Firmware; Software; Operational technology; Supply chain; Acquisition requirements;
7	Estay, D. A. S., & Khan, O. (2016). Control structures in supply chains as a way to manage unpredictable cyber-risks. In *5th World Production and Operations Management Conference*.	Control structures in supply chains as a way to manage unpredictable cyber-risks	2016	It is argued that a systemic approach is more efficient in detecting vulnerabilities, enabling an evolving disruption response process and culture in the supply chain.	Defines feedback loops and control system	**Cyber-Attacks**: Direct attacks on IT systems can disrupt supply chain operations. **Information Flow Disruptions**: Interruptions in information flow can lead to operational failures. **Incorrect Information:** Cyber-attacks can result in the transmission of incorrect information, causing further disruptions. **Delayed Actions**: Cyber-attacks can delay critical actions within the supply chain, leading to inefficiencies.	**Increased Nodes and Connections**: More nodes and connections in the cyber supply chain increase vulnerability. **Anonymity:** Cyber supply chains often involve anonymous interactions, complicating threat detection. **Unlimited Complexity:** The complexity of cyber supply chains is virtually unlimited, making risk management challenging. **Dependence on IT:** Heavy reliance on IT systems introduces new vulnerabilities.	**Complexity:** Traditional risk assessment methods struggle with the increasing complexity of supply chains. **Interaction Failures:** Increased IT integration leads to more interaction failures, which traditional methods often overlook. **Dynamic Nature:** Supply chains are constantly changing, making static risk assessments inadequate. **Resource Intensive:** Traditional methods require significant resources to implement and maintain. **Component vs. Interaction Focus:** Traditional methods focus on component reliability rather than interactions between components.	**Systemic Risk Analysis:** Using systemic methods like STAMP to understand and manage risks. **Feedback Loops:** Implementing feedback loops to monitor and control information flows. **Dynamic Control Structures:** Developing dynamic control structures to adapt to changing conditions. **Continuous Hazard Identification:** Ongoing process of identifying and integrating new hazards into risk management strategies.	Cyber-risks; Supply Chain Management; Resilience;

#	Citation	Title of Papers	Year	Summary	Key take aways	Threats	Sources of Threats	Challenges	Measures	Keywords
8	Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovatio n*, *34*(7), 342-353.	Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems	2014	Discusses the emerging discipline of Cyber Supply Chain Risk Management (CSCRM), highlighting its challenges, threats, sources of threats, and mitigating measures to enhance strategic control over IT systems.	Need for extensive risk practices, communication between departments, suppliers and customers, tough contractual mechanisms and field level strategies for visibility of production/delivery cycles.	**Counterfeits:** Infiltration of counterfeit components into IT systems. **Malicious Tampering:** Embedding of malicious mechanisms in hardware by foreign entities. **Insider Threats:** Fraud and malicious activities by employees within the organization. **Supply Chain Attacks:** Targeting of supply chain contractors and subcontractors by cybercriminals. **Loss of Confidence:** General loss of confidence in technical means to control attacks.	**Foreign Intelligence Services:** Espionage and tampering activities by foreign entities. **Employee Fraud:** Internal fraud and malicious activities by employees. **Cybercriminals:** Cybercriminals targeting supply chain vulnerabilities. **Global Supply Chains:** Increased attack surfaces due to dispersed global supply chains.	**Globalization and Outsourcing:** Rapid globalization and outsourcing of IT systems increase complexity and risk. **Visibility and Control:** Difficulty in gaining visibility and control over extended enterprise partners. **Dynamic Environments:** Addressing the dynamism and real-time scale of adaptive IT networks. **Masked Identities:** Dealing with often unknown supply chain provider identities. **Structural Integration:** Achieving structural integration across the IT supply chain. **Regulatory Compliance:** Navigating complex regulatory requirements and ensuring compliance. **Resource Constraints:** Managing risks with limited resources and budget cuts.	**Risk Assessment Tools:** Development and use of organizational assessment tools and capability/maturity models. **Vendor Audits:** Conducting thorough audits of critical vendors before contract initiation and during yearly reviews. **Contractual Obligations**: Embedding risk management requirements in contracts. **Cross-functional Integration**: Enhancing collaboration between IT, supply chain, and risk management functions. **Continuous Monitoring:** Implementing continuous monitoring and real-time risk dashboards. **Collaboration:** Enhancing collaboration between IT, supply chain, and risk management functions. **Training and Awareness:** Providing training and raising awareness about supply chain risks among employees and partners.	Cybersecurity; Risk management; Supply chain management;
9	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: An International Journal*, *27*(1), 30-53.	Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era	2022	Explores supply chain managers' perceptions of cyber supply chain risk management (CSCRM) and highlights the need for better alignment and holistic strategies to enhance cyber resilience.	Logistics Service Providers can play a crucial role in orchestrating CSCRM efforts across the supply chain, emphasizing the importance of human factors and coordinated, supply chain-wide security strategies.	**ERP Malfunction:** Disruptions caused by enterprise resource planning system failures. **Website Crash:** Impact of website crashes on business operations. **Lack of Connectivity:** Business disruptions due to network connectivity issues. **Malware:** Threats posed by malicious software. **Data Breach:** Risks associated with unauthorized access to sensitive data. **Damage of Records:** Loss or corruption of important records. **Theft of Credentials:** Unauthorized access through stolen credentials.	**Current Employees:** Both intentional and unintentional actions by current employees. **Former Employees:** Risks from former employees with lingering access or knowledge. **Suppliers and Contractors:** Vulnerabilities introduced by third-party suppliers and contractors. **Customers:** Risks from customer interactions and data exchanges. **Hackers/Hacktivists:** External malicious actors targeting the supply chain. **Technical Problems:** Internal and external technical failures affecting operations. **Natural Disasters:** Environmental events disrupting supply chain activities.	**Alignment of Perceptions:** Difficulty in aligning perceptions of cyber risks across different supply chain stages. **Human Factor:** Underestimation of the human factor as a critical element in cyber resilience. **Technical Focus:** Overemphasis on technical solutions rather than holistic, supply chain-wide strategies. **Incident Awareness:** Lack of incident reporting policies leading to low awareness of cyber threats. **Investment Inefficiency:** Inefficient investments due to misaligned perceptions and lack of coordinated efforts.	**Employ a Chief Information Security Officer (CISO) or Data Protection Officer (DPO):** Appointing dedicated officers to oversee cybersecurity. **Conduct Personnel Background Checks:** Ensuring the reliability of employees handling sensitive information. **Presence of an Information Security Strategy:** Developing comprehensive security strategies. **Specific Data and Information Insurance:** Insuring data and information against cyber risks. **Employee Security Awareness Training Program (Cyber Hygiene):** Implementing security awareness programs for employees. **Secure Data Access and Control Measures:** Ensuring secure access and control measures for data. **Accurate Record of Personnel Handling Sensitive Data:** Keeping detailed records of personnel who handle sensitive data. **Intrusion Prevention Systems (IPS), Data and URL Filtering (Antivirus and Antispam):** Utilizing tools like antivirus, antispam, and intrusion prevention systems. **Multiple Data Backup**: Maintaining multiple data backups. **Geographically Distributed Datacentres**: Ensuring data backups are geographically distributed. **Require Suppliers and Customers to Comply with Privacy and Security Policies:** Enforcing compliance with security policies among supply chain partners. **Conduct Supply Chain Partners Security Audits:** Conducting security audits of supply chain partners. **Communication Procedures with Involved Supply Chain Partners:** Establishing communication procedures with supply chain partners during incidents. **Business Continuity and Disaster Recovery Plans:** Establishing disaster recovery and business continuity plans.	Information systems, Resilience, Surveys, Supply-chain management, Risk management, Cyber risk, Information risk, Cyber security;
10	Gani, A. B. D., Fernando, Y., Lan, S., Lim, M. K., & Tseng, M. L. (2022). Interplay between cyber supply chain risk management practices and cyber security performance. *Industri al Management & Data Systems*, *123*(3), 843-861.	Interplay between cyber supply chain risk management practices and cyber security performance	2022	Examines the role of cyber supply chain risk management (CSCRM) practices in achieving supply chain visibility and performance, highlighting the importance of governance, systems integration, and operational processes.	Effective CSCRM practices, particularly governance and systems integration, significantly enhance supply chain visibility, which in turn improves overall cybersecurity performance.	**Cyberattacks:** Various forms of cyberattacks such as phishing, malware, and hacking. **Data Breaches:** Unauthorized access to sensitive information within the supply chain. **Supply Chain Disruptions:** Interruptions caused by cyber incidents affecting supply chain operations.	**Weak Security Controls:** Poor security measures within any network in the supply chain. **Interconnected Systems:** Vulnerabilities arising from the extensive interconnection of systems. **Supplier Networks:** Risks originating from suppliers with inadequate cybersecurity practices. **Technological Changes:** New vulnerabilities introduced by advancements in technology.	**Lack of Visibility:** Difficulty in achieving comprehensive visibility across the supply chain network. **Limited Empirical Data:** Insufficient empirical studies on CSCRM practices and their effectiveness. **Technical Focus:** Predominant focus on technical measures rather than integrating management perspectives. **Operational Bottlenecks:** Challenges in addressing process bottlenecks that hinder operational visibility. **Supplier Integration:** Difficulty in extending cybersecurity measures beyond first-tier suppliers.	**Governance Team:** Establishing a dedicated governance team to oversee cybersecurity practices. **Systems Integration:** Implementing integrated systems for real-time monitoring and decision-making. **Operational Processes:** Developing processes to prevent, detect, and respond to security issues. **Information Sharing:** Enhancing information sharing and collaboration among supply chain partners. **Regular Audits**: Conducting regular audits and compliance checks to ensure adherence to security guidelines.	Cybersecurity, Supply chain visibility, Supply chain risk management, Cyber supply chain risk management;
11	Jazairy, A., Brho, M., Manuj, I., & Goldsby, T. J. (2024). Cyber risk management strategies and integration: toward supply chain cyber resilience and robustness. *Internatio nal Journal of Physical Distribution & Logistics Management*, *54*(11), 1-29.	Cyber risk management strategies and integration: toward supply chain cyber resilience and robustness	2024	Bridges between the established domain of SCRM and the emergent field of SC cybersecurity by forming and testing novel relationships between SCRM-rooted constructs tailored to an SC cyber risks context.	Effective internal and customer cyber integration significantly enhances supply chain cyber resilience and robustness, while supplier integration shows limited impact.	**Cyberattacks:** Various forms of cyberattacks such as phishing, malware, and hacking. **Data Breaches:** Unauthorized access to sensitive information within the supply chain. **Supply Chain Disruptions:** Interruptions caused by cyber incidents affecting supply chain operations.	**Business Partners**: Compromises at business partners can affect the entire supply chain. **Non-Business Entities**: Governments, non-profits, and individuals can be backdoors for cyber threats. **Internal Vulnerabilities**: Weaknesses within the firm's own systems. **External Attackers:** Malicious actors targeting the supply chain.	**Interdependencies**: High interdependencies in supply chains make managing cyber risks complex. **Dynamism**: Rapidly changing cyber threats are difficult to predict and manage. **Anonymity**: Cyber threats often remain undetected until they cause significant damage. **IT Department Involvement**: Requires real-time roles from IT departments, adding complexity. **Ripple Effects**: Cyber threats can quickly spread across interconnected supply chain tiers. **Intentionality**: Most cyber threats are deliberate, requiring proactive measures. **Targeted Assets**: Both physical and information-based assets are at risk.	**Risk Identification**: Identifying potential cyber threats targeting the supply chain. **Risk Protection**: Implementing measures to protect against identified threats. **Risk Detection**: Continuously monitoring for signs of cyber threats. **Risk Response**: Developing plans to respond to cyber incidents. **Risk Recovery**: Establishing procedures to recover from cyberattacks.	Cyberattack, Cybersecurity, Supply chain integration, Relational view, Dynamic capabilities view, Survey;
12	Collier, Z. A., & Sarkis, J. (2021). The zero trust supply chain: Managing supply chain risk in the absence of trust. *International Journal of Production Research*, *59*(11), 3430-3445.	The zero trust supply chain: Managing supply chain risk in the absence of trust	2021	This paper maps zero trust concepts to the supply chain, and discusses the steps an organisation might take to transition to zero trust, and proposes a number of research propositions.	Adopting a zero trust model in supply chain management can significantly enhance security and resilience by addressing the inherent risks and vulnerabilities in modern, interconnected supply chains.	**Supply Chain Attacks**: Infiltration through outside partners or vendors. **Counterfeit Goods**: Entry of counterfeit products posing safety and health risks. **Data Breaches**: Unauthorized access to sensitive information. **Terrorism and Sabotage**: Deliberate acts to disrupt supply chain operations. **Piracy and Theft**: Physical and intellectual property theft. **Industrial Espionage**: Unauthorized access to proprietary information.	**Vendors and Partners**: Vulnerabilities exploited through third-party vendors. **Internal Actors**: Employees or internal systems that may be compromised. **External Actors**: Hackers, terrorists, and other malicious entities. **Technological Systems**: Insecure software and hardware components. **Physical Infrastructure**: Weaknesses in physical distribution and storage systems.	**Complexity of Modern Supply Chains**: Increasing complexity and interconnectedness make it difficult to maintain visibility and traceability. **Dynamic Threat Landscape**: Rapidly evolving tactics and techniques by malicious actors. **Poor Traceability**: Difficulty in tracking and verifying the origins and movements of goods and information. **Trust Issues:** Over-reliance on trust can expose supply chains to more risks. **Implementation of Zero Trust**: Transitioning to a zero trust model requires significant changes in policies and procedures.	**Zero Trust Implementation**: Adopting a zero trust philosophy to assume all actors and activities are untrusted. **Strict Access Control**: Enforcing strict access and authentication requirements. **Continuous Monitoring**: Logging and inspecting all traffic in real-time. **Dynamic Policy Enforcement**: Implementing policies based on continuous, fine-grained data collection and monitoring. **Stakeholder Collaboration**: Engaging all stakeholders in the supply chain to ensure security measures are upheld.	Trust, Risk Management, Security, Supply Chain, Technology Management, Organizational Theory;
13	Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, *13*(1), 103-128.	Cyber security risks in globalized supply chains: conceptual framework	2020	This paper examines the cybersecurity risks in globalized supply chains, categorizes these risks, and proposes a framework for mitigating them.	Identifies and categorizes cybersecurity risks in global supply chains, highlights the importance of managing these risks, and provides strategies for mitigating them to ensure supply chain continuity and security.	**Supply Chain Disruptions**: Interruptions caused by cyber incidents affecting supply chain operations. **Data Theft**: Unauthorized access and theft of sensitive data **Cybercrime**: Criminal activities conducted through cyber means **Malware**: Malicious software disrupting operations **Phishing Attacks**: Fraudulent attempts to obtain sensitive information **Denial of Service Attacks**: Attacks that disrupt service availability **Spoofing Attacks**: Deceptive attacks that falsify data **Direct Attacks:** Direct hacking and data manipulation **Malicious Tampering**: Deliberate tampering with products or data **Fraudulent Communication**: Deceptive communication leading to financial loss **Unauthorized Access**: Gaining unauthorized access to systems **Information Sabotage**: Deliberate sabotage of information systems **Product Specification Fraud**: Fraudulent alteration of product specifications **Counterfeit Products**: Introduction of counterfeit products into the supply chain **Manipulation of Data**: Unauthorized alteration of data **Intellectual Property Theft**: Theft of intellectual property **Unauthorized Access to Customer Data**: Unauthorized access to customer information **Unauthorized Payment Gateways**: Use of unauthorized payment methods	**Insider Threats**: Threats from within the organization. **Cyber Terrorism**: Terrorist activities targeting cyber infrastructure. **Theft of Vendor Credentials**: Stolen credentials leading to unauthorized access **Breach from Vendor Network**: Security breaches originating from vendor networks **Modification of Source Code**: Alteration of source code through malware **Supply of Compromised Software**: Distribution of software with embedded vulnerabilities **Failure to Detect Coding Errors**: Undetected coding errors leading to vulnerabilities	**Lack of Specific Organizational Threat Intelligence**: Difficulty in gathering precise threat intelligence within organizations. **Failure to Audit Third-Party Vendors**: Inadequate auditing of third-party vendors leading to vulnerabilities. **Lack of Security Controls**: Insufficient security controls across the supply chain. **Increased Connectivity Risks**: Higher risks due to increased connectivity in smart manufacturing and supply networks. **Complexity of Cyber-Physical Systems (CPS)**: Managing the complexity and security of CPS. **Insufficient Managerial and Technical Skills**: Lack of skills necessary to implement cybersecurity measures. **Inadequate Standards**: Absence of accurate standards for cybersecurity. **Vulnerabilities in IoT and CPS**: Increased vulnerabilities due to the proliferation of IoT and CPS. **Trust Issues Among Supply Chain Partners**: Lack of trust and cooperation among partners. **Data Privacy Concerns**: Issues related to data privacy in self-thinking supply chains. **Operational Disruptions**: Risks of operational disruptions due to cyber-attacks. **Counterfeit Products**: Risks associated with counterfeit products in the supply chain. **Information Sharing Obstacles**: Challenges in sharing information accurately and securely. **Lack of Transport Encryption**: Absence of encryption during data transport. **Insufficient Authorization**: Inadequate authorization mechanisms leaving systems vulnerable. **Malicious Behavior of Supply Chain Members**: Risks from malicious actions by supply chain members.	**Software Assurance Approach**: Ensuring security, integrity, and authenticity of software. **Data Management**: Implementing effective data management strategies. **Demand-Related Information**: Managing demand information accurately and securely. **Use of Safeguards and Firewalls**: Implementing safeguards and firewalls to protect data. **Adequate Training**: Providing training to handle cybersecurity issues. **Encryption and Coding of Information**: Encrypting and coding information to protect it. **Regular Data Backups**: Regularly backing up commercial data. **Protection from Unauthorized Access**: Implementing measures to prevent unauthorized access. **Strict Password and Account Management**: Enforcing strict password and account management policies. **Inspection and Monitoring**: Regular inspection and monitoring of network components. **Assessment of Cybersecurity Risks**: Assessing potential cybersecurity risks. **Process Monitoring**: Continuous monitoring of processes. **Product Evaluation**: Regular evaluation of products for vulnerabilities. **Integrity Check of Third-Party Products**: Ensuring the integrity of third-party products. **History Check of Network Component Suppliers**: Checking the history of network component suppliers.	Qualitative, Supply chain management, Supply chain, Industry 4.0, Cyber-physical system, Cyber security risks;
14	Eggers, S. (2021). A novel approach for analyzing the nuclear supply chain cyber-attack surface. *Nuclear Engineering and Technology*, *53*(3), 879-887.	A novel approach for analyzing the nuclear supply chain cyber-attack surface	2021	This paper discusses the vulnerabilities and threats in the nuclear supply chain and proposes a novel cyber-attack surface diagram to enhance risk analysis and develop better cybersecurity practices.	Highlights the complexity and vulnerabilities of the nuclear supply chain, emphasizing the need for improved visibility, collaboration, and cybersecurity measures to protect against sophisticated cyber threats.	**Malware Insertion**: Introduction of malicious code into hardware, firmware, or software. **Hardware Tainting**: Compromise of hardware components during manufacturing or distribution. **Component Substitution**: Replacement of genuine components with counterfeit or malicious ones. **Information Falsification**: Alteration of system information to introduce vulnerabilities. **Credential Theft**: Stealing of credentials to gain unauthorized access to systems. **Supply Chain Attacks**: Targeted attacks on the supply chain to introduce persistent threats.	**Nation States:** Countries like China, Russia, Iran, and North Korea are known to engage in cyber espionage and attacks. **Insiders**: Employees or contractors with access to sensitive information can be a source of threats. **Third-Party Vendors**: Suppliers and subcontractors may have less stringent security measures. **Physical and Electronic Channels**: Vulnerabilities exist during the physical and electronic transfer of components and information. **Open-Source and Third-Party Software**: Use of open-source and third-party software introduces risks of compromised code.	**Complexity of the Supply Chain**: The extensive and interconnected nature of the nuclear supply chain makes it difficult to ensure security and authenticity. **Globalization**: The global spread of suppliers increases the risk of compromised components. **Provenance Assurance**: Ensuring the trustworthiness and origin of components is challenging due to the involvement of multiple stakeholders. **Sophistication of Cyber Actors**: Increasingly sophisticated cyber adversaries pose significant threats. **Obsolescence and Modernization**: The transition from analog to digital systems introduces new vulnerabilities. **Limited Visibility**: End users often have limited visibility into the entire supply chain, focusing mainly on first-tier suppliers.	**Cyber-Informed Engineering**: Simplifying designs to reduce the attack surface. **Supply Chain Visibility**: Enhancing visibility into the entire supply chain beyond first-tier suppliers. **Security Certifications**: Limiting purchases to components and systems certified to meet cybersecurity standards. **Industry Collaboration**: Joining data-sharing organizations to share information on supply chain compromises. **Provenance-Aware Supply Chains**: Developing techniques to ensure the authenticity and integrity of components throughout the supply chain. **Enhanced Testing Methods:** Improving testing methods to detect compromised components before installation.	I&C; supply chain; cyber-attack surface;
15	Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Reviewing third-party risk management: best practices in accounting and cybersecurity for superannuation organizations. *Financ e & Accounting Research Journal*, *6*(1), 21-39.	Reviewing third-party risk management: best practices in accounting and cybersecurity for superannuation organizations	2024	Reviews best practices in third-party risk management for superannuation organizations, focusing on accounting and cybersecurity to enhance operational resilience and compliance.	Effective third-party risk management requires thorough due diligence, clear contractual agreements, continuous monitoring, and robust incident response plans to mitigate cybersecurity risks and ensure regulatory compliance.	**Data Breaches**: Unauthorized access to sensitive information. **Cyber Attacks**: Malicious activities targeting third-party vendors. **Operational Disruptions**: Interruptions in services due to cyber incidents. **Financial Losses**: Costs associated with managing and mitigating cyber threats. **Reputational Damage**: Loss of trust and credibility following a cyber incident.	**Third-Party Vendors**: External partners with inadequate cybersecurity measures. **Technological Failures**: Breakdowns in technology infrastructure. **Natural Disasters**: Events causing operational disruptions. **Regulatory Changes**: New laws and standards impacting compliance. **Human Error**: Mistakes made by employees or third-party staff.	**Vendor Selection**: Difficulty in selecting vendors with robust cybersecurity measures. **Contractual Clarity**: Ensuring contracts clearly define roles, responsibilities, and compliance standards. **Continuous Monitoring**: Maintaining ongoing assessment of third-party vendors. **Incident Response**: Developing and testing effective incident response plans. **Regulatory Compliance**: Keeping up with evolving regulatory standards. **Data Security**: Protecting sensitive member data from breaches.	**Due Diligence**: Thorough vetting of third-party vendors. **Contractual Agreements**: Clear contracts outlining cybersecurity expectations. **Regular Audits**: Periodic assessments of vendor compliance. **Continuous Monitoring**: Ongoing evaluation of vendor performance. **Incident Response Plans**: Collaborative development and testing of response strategies. **Employee Training**: Educating staff on cybersecurity risks and protocols.	Third-Party, Risk Management, Superannuation, Cybersecurity, Accounting;

#	Citation	Title of Papers	Year	Summary	Key take aways	Threats	Sources of Threats	Challenges	Measures	Keywords
17	Hammi, B., Zeadally, S., & Nebhen, J. (2023). Security threats, countermeasures, and challenges of digital supply chains. *ACM Computing Surveys*, *55*(14s), 1-40.	Security Threats, Countermeasures, and Challenges of Digital Supply Chains	2023	Discusses the different security issues and attacks that target the different supply chain technologies, and provides some recommendations and best practices that can be adopted to achieve a secure supply chain.	It is paramount to use a hollistic and inte3grated approach to mitigate and inbdentify risks in SCRM	**Malware attacks:** Supply chains are vulnerable to malware such as Mirai, Bashlite, and Mukashi. **DDoS attacks:** Distributed Denial of Service (DDoS) attacks can disrupt supply chain operations. **Counterfeit components:** Fake hardware and software introduce security and safety risks. **Insider threats:** Authorized users may misuse access to compromise the supply chain. **Supply chain poisoning:** Malicious actors inject vulnerabilities into software and hardware before distribution. **Third-party dependencies:** Weak links in third-party vendors create cascading security failures. **Malicious Tampering:** Intentional tampering with IT products by adversaries.	**Hardcoded credentials;** Default credentials in devices and software lead to easy exploitation. **Social engineering risks:** Phishing and impersonation attacks target human vulnerabilities within the supply chain. **Authentication weaknesses:** Many supply chain systems suffer from weak authentication and access controls. **Third-party suppliers:** External vendors introduce unknown risks and vulnerabilities. **Nation-state actors:** Governments may exploit supply chains for espionage or cyber warfare. **Criminal organizations:** Cybercriminals seek financial gains by targeting supply chains. **Insider threats:** Employees or contractors with privileged access may intentionally or unintentionally cause security breaches. **Open-source vulnerabilities:** Unverified code in software supply chains can be exploited. **Foreign Intelligence Services:** Espionage activities by foreign entities.	**Lack of visibility:** Organizations lack full control over supply chain ecosystems, leading to blind spots in security. **Fragmented security approaches:** Poor coordination between suppliers and customers results in unaligned security measures. **Reliance on common components:** Shared software, hardware, and firmware across industries create systemic vulnerabilities. **Globalization and Outsourcing:** Increased complexity and risk due to the rapid globalization and outsourcing of IT systems. **Regulatory Compliance:** Meeting diverse regulatory requirements is challenging and costly. **Dynamic Threat Environment:** Adapting to constantly evolving and sophisticated cyber threats.	**Organizational Measures** **Develop Threat Models:** Organizations should create robust threat models to accurately assess supply chain risks, avoiding reliance solely on proprietary models. **Independent Audits**: Regular third-party audits should be conducted to provide an unbiased security evaluation, despite potential cost and time constraints. **Governmental Supervision**: Regulatory bodies should oversee supply chain security, though scalability remains a challenge. **Formal Risk Management Programs**: Establish formal programs with governance, policies, and tools to ensure accountability in cyber supply chain risk management (CSCRM). **Supplier Risk Assessment**: Organizations must identify, assess, and continuously monitor critical suppliers to ensure security compliance. **Supply Chain Mapping**: Maintain full visibility into all components of the supply chain to identify weak links. **Collaboration with Key Suppliers**: Foster close relationships with critical suppliers to enhance security measures and integrate resilience efforts. **Technical Measures** **Blockchain for Supply Chain Security**: Utilize blockchain technology for traceability, immutability, and data integrity, ensuring a secure record of supply chain transactions. **Strong Authentication Mechanisms**: Implement multi-factor authentication (MFA) and digital signatures to prevent unauthorized access. **Elliptic Curve Cryptography (ECC)**: Use lightweight ECC techniques for resource-constrained IoT devices to enhance encryption without high computational overhead. **Digital Signature Algorithms**: Deploy secure authentication and data integrity mechanisms such as the Elliptic Curve Digital Signature Algorithm (ECDSA). **Timestamp Verification**: Introduce timestamp verification to mitigate replay attacks in data transmission. **Decentralized Certification Mechanisms**: Implement blockchain-based certification mechanisms to provide lightweight security certificates for IoT devices. **Physically Unclonable Functions (PUF)**: Use PUF technology as an alternative for device authentication in cases where blockchain-based certification is not feasible. **Industry-Specific Security Solutions** **Trusted Execution Environments (TEEs):** Secure supply chain transactions using TEEs and smart contracts, despite potential latency challenges. **RFID-Based Product Ownership Management (POMS)**: Enhance anti-counterfeiting measures by leveraging blockchain-based RFID authentication. **IoT-Integrated Blockchain Systems**: Use secure two-way authentication and encryption in IoT-based blockchain systems for supply chain monitoring. **Trust Management Frameworks**: Implement blockchain-based trust management frameworks like TrustChain to dynamically assign trust and reputation scores.	Blockchain, CPS, Countermeasures, Cyberattacks, IIoT, issues, Supply chain cybersecurity;
18	PN, S., & Kunnathur, A. S. (2015). Information security in supply chains: A management control perspective. *Informati on & Computer Security*, *23*(5), 476-496.	Information security in supply chains: a management control perspective	2015	The need for management control system for information security management that encapsulates the technical, formal and informal systems and the importance of having a higher level of control above the already existing levels	Cyber supply chain security requires a holistic approach that integrates management control mechanisms, standardized policies, and proactive risk management to address inter-organizational vulnerabilities	**Human Errors**: Mistakes made by employees that can lead to security breaches. **Insider Threats**: Malicious actions by trusted personnel within the organization. **External Attacks**: Cyber-attacks from external sources targeting the supply chain. **Technological Vulnerabilities**: Weaknesses in the technical infrastructure that can be exploited. **Inter-organizational Communication**: Security risks arising from informal and uncontrolled communication between organizations.	**Unsecured Informal Communication:** Information leaks through casual conversations, emails, or unsecured networks. **Lack of Interoperable Security Measures:** Variability in security implementations across partners creates gaps. **Inadequate Access Control**: Weak authentication and authorization measures expose systems to attacks. **Weak Governance of Third-Party Risks:** Security breaches at suppliers or partners affect the entire chain. **Lack of Security Awareness:** Employees unaware of security protocols may unintentionally compromise information. **Weak Policy Enforcement:** Poor governance leads to inconsistent application of security measures. **Cross-Border Supply Chain Risks:** Legal and regulatory inconsistencies increase security challenges.	**Organizational Composition and Infrastructure: Difficulty** in enforcing controls across varied organizational structures within the supply chain. **Security Culture**: Ensuring a consistent security culture across different organizations and cultural contexts. **Security Policy**: Developing and aligning security policies across multiple organizations in the supply chain. **Security Strategy**: Creating a comprehensive, multilateral security strategy that addresses both intra- and inter-organizational security needs. **Information Security Standards and Practices**: Standardizing security practices across different organizations to handle communication breakdowns and security breaches. **Power and Control**: Managing skewed power dynamics and control structures within the supply chain to ensure effective security.	**Technical Controls** **Firewalls**: Protect the network by controlling incoming and outgoing network traffic based on predetermined security rules. **Antivirus Applications**: Detect and remove malicious software to protect the system from viruses and malware. **Biometric Devices**: Use unique biological traits (e.g., fingerprints, retina scans) for authentication and access control. **Digital Signatures**: Ensure the authenticity and integrity of digital messages or documents. **Voice Analysis**: Authenticate users based on their voice patterns. **Authentication Protocols**: Implement protocols to verify the identity of users accessing the system. **Access Control Mechanisms**: Use passwords, biometric controls, and other methods to ensure only authorized personnel can access sensitive information. **Network Security Controls**: Set up measures to protect the network from unauthorized access and threats. Cryptographic Techniques: Use encryption to secure data during transmission and storage. **Formal Controls** **Security Policies**: Develop and enforce policies that dictate how technical controls are implemented and used. **Guidelines for Inter-organizational Information Transfer**: Standardize security policies across organizations in the supply chain to ensure secure information sharing. **Documentation of Security Issues**: Address and document potential security issues arising from logistics, employee transfer/termination, power, and control. **Role and Responsibility Allocation**: Clearly define and allocate responsibilities for security within the organization. **Consequences of Role Deviance**: Establish consequences for misinterpretation of data and misapplication of rules. **Informal Controls** **Training Programs**: Conduct training sessions to educate employees about information security measures. **Awareness Programs**: Foster a security culture by raising awareness about security issues and best practices. **Cultural Climate Development**: Create a cultural climate that motivates employees to follow formal and technical security policies. **Open Lines of Communication**: Ensure open communication between managerial and security personnel to identify potential vulnerabilities and mitigate risks. **Management Controls** **Integration and Coordination**: Manage the generation and distribution of information to ensure accurate and complete information flow for all supply chain activities. **Motivation of Managers**: Encourage managers to implement and execute information security initiatives that benefit the entire supply chain. **Strategic Security Objectives**: Align management control systems with the achievement of strategic security objectives. **Governance Structure**: Define a governance structure that includes security practices regulating lateral relations across organizational boundaries. **Monitoring Informal Interactions**: Oversee informal interactions between organizations in the supply chain to ensure security. **Collaboration with Third-party Security Providers**: Work with third-party security providers to secure information flows between supply chain organizations.	Supply chain, Information security, Management control, Informal control, Formal control, Technical control;
20	Adenekan, O. A., Ezeigweneme, C., & Chukwurah, E. G. (2024). Strategies for protecting IT supply chains against cybersecurity threats. *International Journal of Management & Entrepreneurship Research*, *6*(5), 1598-1606.	Strategies for protecting IT supply chains against cybersecurity threats	2024	Underscores the evolving nature of cyber threats and the imperative for adaptive strategies, and calls for concerted efforts from businesses, policymakers, and IT professionals to prioritize and continuously refine cybersecurity measures in safeguarding IT supply chains against future threats.	Highlights the critical importance of a proactive and comprehensive approach to cybersecurity in IT supply chains, involving risk management, international standards, vendor management, and advanced technologies to safeguard against evolving cyber threats	**Phishing Schemes**: Sophisticated phishing attacks targeting supply chain employees. **Ransomware**: Attacks locking critical data and systems until a ransom is paid. **State-Sponsored Espionage**: Espionage activities by state-sponsored actors to steal intellectual property or disrupt operations.	**Software Development**: Vulnerabilities in software, including third-party libraries or open-source components. **Third-Party Vendors**: Security posture and data handling practices of third-party vendors. **Hardware Components**: Counterfeit components and vulnerabilities within microchips and firmware.	**Vulnerability Points**: Multiple software, hardware, and service layers each have unique vulnerabilities. **Third-Party Risks**: Reliance on third-party vendors introduces additional risks due to varying security postures. **Hardware Vulnerabilities**: Counterfeit components and vulnerabilities within microchips and firmware. **Complexity**: The intricate and interconnected nature of IT supply chains increases the difficulty of securing them.	**Risk Assessment and Management** **Identifying Risks**: Conduct a thorough inventory of all assets within the supply chain and identify potential threats, including software vulnerabilities, hardware tampering, insider threats, and third-party service provider risks. **Analyzing Risks**: Analyze identified risks to understand their potential impact and likelihood, prioritizing them based on severity. **Prioritizing and Mitigating Risks**: Implement security controls, develop incident response plans, and establish continuous real-time monitoring mechanisms to detect and respond to threats. **Implementation of Security Standards and Frameworks** **ISO/IEC 27001**: Adopt this international standard for establishing, implementing, maintaining, and continuously improving an information security management system (ISMS), emphasizing risk management. **NIST Cybersecurity Framework**: Utilize this framework to assess and improve the ability to prevent, detect, and respond to cyber attacks, adapting its principles to secure the IT supply chain. **Enhanced Vendor Management** **Due Diligence**: Conduct thorough assessments of vendors' security postures, compliance with relevant standards, and history of security incidents before engagement. **Ongoing Audits**: Regularly audit third-party vendors to ensure compliance with security requirements and standards, identifying vulnerabilities in their operations. **Contractual Security Requirements**: Include explicit security requirements in contracts with third-party vendors, covering compliance with standards, incident reporting protocols, and the right to audit. **Advanced Security Technologies** **Blockchain for Secure Transaction Logging**: Implement blockchain technology for decentralized and tamper-proof logging of transactions and interactions within the supply chain. **AI and Machine Learning for Threat Detection**: Use AI and machine learning algorithms to analyze data and identify patterns indicative of malicious activity, enabling early threat detection. **Secure Access Controls**: Implement multi-factor authentication (MFA), role-based access control (RBAC), and identity and access management (IAM) systems to ensure only authorized individuals can access critical assets. **Best Practices in IT Supply Chain Security** **Zero-Trust Security Model**: Adopt a zero-trust model that requires strict identity verification, access control, and continuous monitoring of network activities. **Regular Security Training for Employees**: Conduct regular security awareness training to educate employees on the latest cyber threats, safe online practices, and the importance of adhering to security policies. **Secure Software Development Practices**: Incorporate secure development practices, such as code reviews, automated testing, and vulnerability assessments, throughout the software development lifecycle (SDLC).	IT Supply Chain, Cybersecurity, Risk Management, Blockchain, Zero-Trust Model, Artificial Intelligence;

#	Citation	Title of Papers	Year	Summary	Key take aways	Threats	Sources of Threats	Challenges	Measures	Keywords
21	Cheung, K. F., Bell, M. G., & Bhattacharjya, J. (2021). Cybersecurity in logistics and supply chain management: An overview and future research directions. Transportation Research Part E: Logistics and Transportation Review, 146, 102217.	Cybersecurity in logistics and supply chain management: An overview and future research directions	2021	The paper reviews cybersecurity measures in logistics and supply chain management, highlighting challenges, threats, sources of threats, and mitigating measures, with a focus on the need for real cybersecurity data, methodological diversity, and advanced technologies like blockchain and quantum-safe cryptography.	Importance of real cybersecurity data, the need for more quantitative and diverse research methodologies, the early stage of blockchain adoption, and the critical role of advanced encryption and digital forensic investigation in enhancing cybersecurity in logistics and supply chain management.	**Data Leakage**: Unauthorized access and exposure of sensitive information. **Malware and Ransomware Attacks**: Disruptive software that can damage or disable systems. **Supply Chain Vulnerabilities**: Weaknesses in the supply chain that can be exploited by cybercriminals. **Legacy Systems**: Outdated systems that are more susceptible to cyberattacks. **Insufficient Cybersecurity Awareness**: Lack of knowledge and training among staff regarding cybersecurity threats.	**Cybercriminals**: Individuals or groups with malicious intent to exploit vulnerabilities. **Insider Threats**: Employees or partners who may intentionally or unintentionally cause security breaches. **Technological Advancements**: Rapid development of technologies like quantum computing that can render current security measures obsolete. **Complex Supply Chains**: The interconnected nature of modern supply chains increases the attack surface.	**Lack of Real Cybersecurity Data**: Difficulty in obtaining real-world cybersecurity data for research purposes. **Scarcity of Studies on Cybersecurity in Logistics**: Limited research focused specifically on logistics within the broader supply chain context. **Lack of Methodological Diversity**: Predominance of qualitative studies, indicating the field is still emerging. **Insufficient Focus on Real-Time Recovery and Aftermath Measures**: Most studies emphasize precautionary measures over real-time recovery and aftermath strategies. **Early Stage of Blockchain Adoption**: Blockchain technologies are still in their infancy in the transport and logistics sector. **Limitations of Current Encryption Schemes**: Existing encryption methods may become vulnerable with the advancement of quantum computing. **Scarcity of Studies on Information Security and Digital Forensic Investigation**: Limited research on these critical areas.	**Precautionary Measures** **Access Control**: Implementing measures to restrict access to sensitive information and systems. **Authentication**: Using multi-factor authentication protocols, including biometric authentication mechanisms. **Certified Hard- and Software**: Ensuring that risk identification software is certified or purchased from trusted vendors. **Counterfeit Prevention**: Implementing measures to prevent counterfeit hardware and software. **Data Protection**: Using blockchain and encryption to secure data and ensure its integrity. **Firewall and Gateway**: Installing trusted firewalls and gateways to protect the network. **Information Sharing**: Establishing secure information sharing schemes among supply chain partners. **Laws, Policies, Regulations, and Standards**: Developing and adhering to cybersecurity guidelines and standards. **Regular Patching and Updating**: Ensuring systems are regularly patched and updated to protect against vulnerabilities. **Risk/Vulnerability Identification**: Implementing software and methodologies to identify and mitigate risks. **Supplier Auditing**: Regularly auditing suppliers to ensure they meet cybersecurity standards. **Supply Chain Partner Collaboration**: Collaborating with supply chain partners to maintain network availability and connectivity. **Staff Training and Hiring Skilled Cybersecurity Workforce**: Educating and employing knowledgeable staff to handle cybersecurity threats. **Real-Time Recovery Measures** **Component Recovery**: Recovering compromised components during an attack. **Component Isolation**: Isolating compromised components to prevent damage propagation. **Real-Time Monitoring**: Continuously monitoring systems to detect and respond to threats. **Supply Chain Partner Interaction**: Communicating with supply chain partners to mitigate the impact of ongoing cyberattacks. **Task Force**: Allocating task forces to ensure recovery of compromised components. **Aftermath Measures** **Behavior Analysis and Feedback**: Analyzing system behavior and providing feedback to refine recovery measures. **Collaborative Recovery Plan Process with Supply Chain Partners**: Developing and implementing recovery strategies with supply chain partners. **Data Backup**: Implementing data restoration protocols using the latest backups. **Digital Forensic Investigation**: Investigating breaches to understand and mitigate vulnerabilities. **Insurance**: Having appropriate insurance cover to make claims during the aftermath of an attack. **Recovery Plan Procedures**: Initiating recovery procedures to restore affected systems to a fully functional state. **Resilient Infrastructure Design**: Designing resilient infrastructure to enhance recovery speed. **System Restoration**: Restoring systems to a fully functional state after an attack.	Cybersecurity; Defensive measures; IoT; Blockchain; Logistics; Supply chain;
22	Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. *Electronics*, *9*(11), 1864.	Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions	2020	The nature of the military supply chains 4.0 is explained and how it uniquely differs from the commercial supply chain, revealing their strengths, weaknesses, dependencies and the fundamental technologies upon which they are built.	The critical need for robust cybersecurity measures, regular risk assessments, and collaboration with suppliers to mitigate the risks associated with the integration of emerging technologies in modern supply chains.	**Cyber-Attacks**: Increasing sophistication and frequency of cyber-attacks targeting supply chains. **Data Breaches**: Unauthorized access to sensitive information within the supply chain. **Advanced Persistent Threats (APTs)**: Long-term, targeted cyber-attacks aimed at stealing data or disrupting operations. **Supply Chain Poisoning**: Introduction of malicious components or software into the supply chain. **Operational Disruptions**: Interruptions caused by cyber incidents affecting supply chain operations.	**External Suppliers**: Risks from third-party vendors and suppliers with less secure systems. **Interconnected Systems**: Vulnerabilities arising from the integration of multiple systems and networks. **Legacy Systems**: Older systems that are more susceptible to cyber-attacks. **Human Factors**: Insider threats and human errors that can compromise security. **Emerging Technologies**: New technologies that introduce unknown vulnerabilities.	**Lack of Semantic Standards**: Inconsistent data formats and terminologies hinder effective communication and integration. **Poor Interoperability**: Difficulty in integrating diverse systems and technologies within the supply chain. **Security Gaps**: Inadequate security measures in manufacturing and IT processes. **Complexity of Systems**: Managing the complexity of interconnected systems and networks. **Dependency on Emerging Technologies**: Reliance on technologies like blockchain and IoT, which introduce new vulnerabilities.	**Enhanced Cybersecurity Protocols** **Encryption**: Use of cryptographic techniques to protect data integrity and confidentiality. **Multi-Factor Authentication (MFA)**: Implementing MFA to ensure secure access to systems. **Regular Software Updates**: Ensuring all systems and software are up-to-date with the latest security patches. **Network Segmentation**: Dividing networks into segments to limit the spread of cyber-attacks. **Intrusion Detection Systems (IDS):** Deploying IDS to monitor and detect suspicious activities. **Regular Risk Assessments** **Vulnerability Assessments**: Conducting regular assessments to identify and address vulnerabilities. **Penetration Testing**: Simulating cyber-attacks to test the effectiveness of security measures. **Risk Analysis Frameworks**: Utilizing frameworks like Crown Jewel Analysis and Supply Chain Resilience Framework to assess risks. **Continuous Monitoring**: Implementing continuous monitoring of systems to detect and respond to threats in real-time. **Supply Chain Visibility** **Track and Trace Systems**: Using technologies like RFID and 5G to monitor the movement of goods in real-time. **Blockchain Technology**: Implementing blockchain for secure and transparent transactions within the supply chain. **Smart Contracts**: Utilizing smart contracts to automate and enforce agreements within the supply chain. **Data Analytics**: Leveraging data analytics to gain insights into supply chain operations and identify potential risks. **Collaboration with Suppliers** **Supplier Audits**: Conducting regular audits of suppliers to ensure they adhere to security standards. **Information Sharing**: Establishing mechanisms for sharing threat intelligence and best practices with suppliers. **Joint Security Exercises**: Collaborating with suppliers to conduct joint security exercises and improve overall resilience. **Standardized Security Protocols**: Developing and enforcing standardized security protocols across all suppliers. **Adoption of Advanced Technologies** **Artificial Intelligence (AI)**: Using AI to enhance threat detection and response capabilities. **Internet of Things (IoT)**: Integrating IoT devices for improved monitoring and control of supply chain operations. **Cyber-Physical Systems (CPS)**: Implementing CPS to enhance the interaction between physical and digital systems. **Fog Computing**: Utilizing fog computing to process data closer to the source, reducing latency and improving security. **Additional Measures** **Business Continuity Planning**: Developing and maintaining business continuity plans to ensure operations can continue during and after a cyber incident. **Employee Training**: Providing regular training to employees on cybersecurity best practices and awareness. **Incident Response Plans**: Establishing and regularly updating incident response plans to quickly address and mitigate cyber incidents. **Redundancy and Backup Systems**: Implementing redundancy and backup systems to ensure data and system availability in case of an attack.	cyber security; semantic systems; supply chain 4.0; blockchain; cyber-physical systems;

Appendix D

Coding (sub-)categories concepts

Table D.1 presents the different concepts identified during the expert interviews structured in (sub-)categories.

Category	Subcategory	Concept
Challenges in C-SCRM	Resource Constraints	Insufficient internal resources dedicated to C-SCRM programs.
Challenges in C-SCRM	Resource Constraints	Limited staff, budget, or expertise available for C-SCRM initiatives.
Challenges in C-SCRM	Resource Constraints	Heavy reliance on external support due to internal resource shortages.
Challenges in C-SCRM	Governance & Ownership	Unclear internal ownership for third-party cyber risk management.
Challenges in C-SCRM	Governance & Ownership	No single department or role responsible for C-SCRM oversight.
Challenges in C-SCRM	Cross-Functional Coordination	Difficulty coordinating across multiple departments for C-SCRM implementation.
Challenges in C-SCRM	Cross-Functional Coordination	Managing collaboration between departments like IT, procurement, and legal.
Challenges in C-SCRM	Cross-Functional Coordination	Implementing C-SCRM requires involvement of multiple departments, which is complex.
Challenges in C-SCRM	Scalability & Data Visibility	Difficulty in scaling risk management to thousands of suppliers.
Challenges in C-SCRM	Scalability & Data Visibility	Lack of centralized data management for supplier information.
Challenges in C-SCRM	Scalability & Data Visibility	Siloed systems and decentralized procurement hinder supplier data visibility.
Challenges in C-SCRM	High Dependency (SME Perspective)	Small organizations often rely heavily on a few critical suppliers.
Challenges in C-SCRM	High Dependency (SME Perspective)	Small organizations may have limited alternatives to critical suppliers.
Challenges in C-SCRM	High Dependency (SME Perspective)	Small organizations often lack exit plans or backup options for critical suppliers.
Challenges in C-SCRM	Value Realization	Difficulty in translating supplier risk assessments into actionable steps.
Challenges in C-SCRM	Value Realization	C-SCRM programs often identify risks but lack mechanisms to mitigate them.
Challenges in C-SCRM	Value Realization	It's hard to justify the effort of conducting supplier risk assessments without clear mitigation actions.
Challenges in C-SCRM	Technology Limitations	Existing tools and technology are insufficient for C-SCRM needs.
Challenges in C-SCRM	Technology Limitations	C-SCRM processes remain fragmented across multiple systems.
Challenges in C-SCRM	Technology Limitations	Anticipated solutions like AI for contract review are still developing and not yet meeting expectations.
Risk Concerns	Supplier Cyber Incidents	Data breaches or cyber-attacks at a supplier that compromise the organization's data or services.
Risk Concerns	Supplier Cyber Incidents	If a vendor fails to protect information, the client organization suffers damage.
Risk Concerns	Operational Disruption	Business continuity failures caused by third-party issues.
Risk Concerns	Operational Disruption	Outages caused by a critical service provider going down, impacting operations.
Risk Concerns	Regulatory/Compliance Impact	Non-compliance or regulatory penalties from supplier failings.
Risk Concerns	Regulatory/Compliance Impact	New regulations (NIS2, DORA) require control over supplier risk, making incidents lead to legal violations.
Risk Concerns	Multi-Tier & Concentration Risk	Risks from fourth- and fifth-party suppliers.
Risk Concerns	Multi-Tier & Concentration Risk	Vendor concentration issues when using many vendors relying on the same sub-provider.

Risk Concerns	Vendor Lock-In	Being dependent on a dominant supplier (e.g. cloud or IT provider).
Risk Concerns	Vendor Lock-In	Lack of influence over a dominant supplier's security posture.
Risk Concerns	Vendor Lock-In	Accruing risk by trusting large vendors (e.g. Microsoft) despite known security issues.
Risk Concerns	Third-Party Access Risk	Security risks from external vendors accessing internal systems.
Risk Concerns	Third-Party Access Risk	Risks of external vendors accessing operational technology (OT) systems.
Risk Concerns	Third-Party Access Risk	Vendors with privileged access to systems, introducing vulnerabilities.
Mitigation Measures	Governance Structure	Establish a cross-functional supply chain risk council to define roles and responsibilities.
Mitigation Measures	Governance Structure	Ensure departments like IT, security, procurement, and legal are involved in C-SCRM governance.
Mitigation Measures	Policy & Standards	Develop a comprehensive C-SCRM policy and framework of standards/procedures.
Mitigation Measures	Policy & Standards	Classify vendors by criticality and risk tier, with defined assurance levels for each tier.
Mitigation Measures	Supplier Risk Assessment	Conduct security questionnaires, reviews, or certifications for suppliers.
Mitigation Measures	Supplier Risk Assessment	Use standardized tools or frameworks (e.g. ISO, NIST) for supplier assessments.
Mitigation Measures	Supplier Risk Assessment	Adjust risk assessments based on supplier context.
Mitigation Measures	Tiered Assurance & Tailoring	Allocate assurance activities based on supplier risk tier.
Mitigation Measures	Tiered Assurance & Tailoring	High-risk vendors should undergo deeper assessments, audits, or certifications.
Mitigation Measures	Tiered Assurance & Tailoring	Special controls may be needed for atypical vendors, like small vendors with privileged access.
Mitigation Measures	Contractual Controls	Embed security requirements into supplier contracts.
Mitigation Measures	Contractual Controls	Include clauses for data protection, audits, incident reporting, and liability for security failures.
Mitigation Measures	Contractual Controls	Use contractual leverage to enforce improvements and penalties for security failures.
Mitigation Measures	Auditing & Monitoring	Perform regular supplier audits (on-site or remote assessments of controls).
Mitigation Measures	Auditing & Monitoring	Negotiate audit rights for suppliers to ensure audits can be conducted without cost to the client.
Mitigation Measures	Auditing & Monitoring	Critical suppliers should be audited to drive remediation of issues.
Mitigation Measures	Access Management (OT & IT)	Implement strict controls for third-party access to systems.
Mitigation Measures	Access Management (OT & IT)	Maintain an inventory of suppliers with network access.
Mitigation Measures	Access Management (OT & IT)	Use privileged access management tools for vendor connections.
Mitigation Measures	Access Management (OT & IT)	Enforce network segmentation to limit the blast radius of third-party accounts.

Mitigation Measures	Incident Planning & Exit Strategy	Develop and test incident response plans that include suppliers.
Mitigation Measures	Incident Planning & Exit Strategy	Ensure contracts stipulate incident notification procedures.
Mitigation Measures	Incident Planning & Exit Strategy	Maintain exit strategies for critical suppliers, including alternative suppliers or contingency plans.
Mitigation Measures	Tooling & Automation	Use technology platforms for vendor risk management, contract analysis, and threat intelligence.
Mitigation Measures	Tooling & Automation	Consider managed services or external support to fill resource gaps, but ensure oversight.
Limitations of Existing C-SCRM Guidance	Fragmentation of Frameworks	Lack of a single, cohesive industry standard for C-SCRM.
Limitations of Existing C-SCRM Guidance	Fragmentation of Frameworks	Existing C-SCRM guidance is spread across various standards (NIST, ISO, etc.).
Limitations of Existing C-SCRM Guidance	Poor Adoption by Industry	C-SCRM-specific frameworks (e.g. NIST SP 800-161) are not widely adopted, especially by smaller organizations.
Limitations of Existing C-SCRM Guidance	Poor Adoption by Industry	No broadly accepted certification for C-SCRM exists, unlike ISO 27001.
Limitations of Existing C-SCRM Guidance	Theoretical & Vague Guidance	Existing C-SCRM guidelines tend to be high-level and theoretical.
Limitations of Existing C-SCRM Guidance	Theoretical & Vague Guidance	Guidance lacks concrete operational details on how to implement C-SCRM processes.
Limitations of Existing C-SCRM Guidance	Outdated Focus	Existing standards do not sufficiently account for evolving technology and threats (e.g. AI, cloud ecosystems).
Limitations of Existing C-SCRM Guidance	Usability Challenges	C-SCRM guidance is often lengthy and difficult to navigate.
Limitations of Existing C-SCRM Guidance	Usability Challenges	Interpreting regulatory texts (e.g. DORA RTS, NIS2) requires significant expertise.
Limitations of Existing C-SCRM Guidance	Usability Challenges	The complexity of guidance makes implementation daunting for organizations with limited cybersecurity maturity.

Limitations of Existing C-SCRM Guidance	Lack of Examples & Tools	Existing frameworks often do not mention specific tools or solutions for C-SCRM.
Limitations of Existing C-SCRM Guidance	Lack of Examples & Tools	Smarter solutions exist for C-SCRM challenges but are not referenced in standard best-practice documents.
Feedback on Proposed Guideline	Holistic Scope Clarification	Define the term "holistic approach" clearly in the guideline.
Feedback on Proposed Guideline	Holistic Scope Clarification	Clarify that the guideline requires cross-domain involvement beyond cybersecurity, including operational, financial, and legal risks.
Feedback on Proposed Guideline	Cross-Functional Involvement	Ensure all relevant departments are included in C-SCRM processes.
Feedback on Proposed Guideline	Cross-Functional Involvement	Emphasize that C-SCRM should involve procurement, legal, and other departments, not just the security team.
Feedback on Proposed Guideline	Regulatory Communication	Expand the guideline's communication and reporting section to include external notifications.
Feedback on Proposed Guideline	Regulatory Communication	Ensure the guideline covers legally required disclosures, such as reporting incidents to regulators or informing clients.
Feedback on Proposed Guideline	Training Coverage	Clarify the scope of training programs to include contractors and suppliers.
Feedback on Proposed Guideline	Training Coverage	Mention expectations for third-party personnel training, especially for key suppliers.
Feedback on Proposed Guideline	Format & Presentation	Ensure the guideline is accessible to decision-makers.
Feedback on Proposed Guideline	Format & Presentation	Present the guideline in an engaging format (e.g. visual roadmap, concise deck) to improve executive acceptance.
Feedback on Proposed Guideline	Actionability & Depth	Ensure the guideline provides practical tips and tricks to facilitate implementation.
Guideline Evaluation (FACE)	Feasibility	Implementing the guideline is feasible but resource-dependent.
Guideline Evaluation (FACE)	Feasibility	Successful implementation of the guideline requires sufficient staffing and budget.
Guideline Evaluation (FACE)	Feasibility	Limited organizational capacity is a barrier to full implementation.
Guideline Evaluation (FACE)	Acceptability	High acceptability, especially among risk and security professionals.
Guideline Evaluation (FACE)	Acceptability	Decision-makers may not engage with a lengthy document, so communication format is key.

Guideline Evaluation (FACE)	Cost	Perceived cost is moderate and justifiable.
Guideline Evaluation (F.A.C.E.-IT)	Cost	The guideline's recommendations are mostly process-oriented and not costly.
Guideline Evaluation (FACE)	Cost	C-SCRM programs are resource-intensive by nature, but the guideline does not add significant costs.
Guideline Evaluation (FACE)	Equity (Large vs Small)	Mixed impact on small organizations; some find the guideline beneficial, others see added work.
Guideline Evaluation (FACE)	Equity (Large vs Small)	The guideline can level the knowledge gap but may not overcome the resource gap between large and small organizations.
Guideline Evaluation (FACE)	Intent to Implement	Strong intent to adopt and integrate the guideline's recommendations.
Guideline Evaluation (FACE)	Intent to Implement	Experts see tangible value in the guideline and are eager to implement it.

Table D.1: Overview of the (sub-)categories and concepts collected from the expert interviews.

Acronyms

APTs Advanced Persistent Threats. 26

BCP Business Continuity Planning. 60, 61

BIA Business Impact Analysis. 39

C-SCRM Cyber Supply Chain Risk Management. 1, 5–9, 11–13, 15–18, 21–25, 27, 29–38, 41–46, 48–53, 55–58, 61, 63, 64, 66, 68, 69, 71, 74, 75, 78, 79, 84, 87, 92, 101–103, 111, 112

DDoS Distributed Denial-of-Service. 26, 28

DORA Digital Operational Resilience Act. 18, 32, 38, 109

DR Disaster Recovery. 60, 61

DSRM Design Science Research Methodology. 103

EOL end-of-life. 65

ESAs European Supervisory Authorities. 12

ICT Information and Communication Technology. 38

IoT Internet of Things. 16, 21

IR Incident Response. 60, 61

ISMS Information Security Management System. 35

ISO International Organization for Standardization. 1, 5, 12

IT Information Technology. 4, 21, 126

MITM Man-in-the-Middle. 26

NIS2 Network and Information Systems Directive 2. 1, 4–6, 8, 18

NIST National Institute of Standards and Technology. 1, 5, 12, 21, 31–33

OT Operational Technology. 4, 21, 126

RTS Regulatory Technical Standards. 13, 15, 18, 32, 33, 38–40, 109, 110

SBOMs Software Bills of Materials. 75

SCADA Supervisory Control and Data Acquisition. 28

SCRM Supply Chain Risk Management. 4, 9, 21, 22

SDLC Software Development Life Cycle. 49, 50

SMEs Small and Medium Enterprises. 25, 103

SOC Security Operations Center. 70

TPRM Third-Party Risk Management. 9

List of terms

Advanced Persistent Threats Long-term, targeted cyberattacks by skilled adversaries aiming to steal data or disrupt operations.. 26, 124

Cyber Supply Chain Risk Management The process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of IT/OT product and service supply chains. [56]. 1, 5, 21, 22, 102, 103, 111, 124

cybersecurity The practice of protecting systems and information from digital attacks or mitigating their impact [44]. 4, 5, 21–23

Distributed Denial-of-Service A cyberattack where multiple compromised systems flood a target with traffic, overwhelming it and causing service disruptions or outages.. 26, 124

Industry 4.0 The fourth industrial revolution, characterized by the integration of digital technologies with industrial processes. 4

KPMG Klynveld Peat Marwick Goerdeler, a global network of professional services firms. 6, 17

Malware A portmanteau of "malicious software", referring to software designed to cause damage, disruption or unauthorized access to an automated work.. 26

Man-in-the-Middle A cyberattack where an attacker secretly intercepts and possibly alters the communication between two parties (or systems) who believe they are directly communicating with each other.. 26, 124

Phishing Form of social engineering and a fraudulent practice aimed at deceiving people into revealing sensitive information or installing malware.. 26

SOC 2 report Audit report assessing a service provider's controls for security, availability, confidentiality, and privacy, based on the AICPA's Trust Services Criteria. [4] . 37, 55, 57, 81, 96, 97

Software Development Life Cycle A process used by software developers to design, develop, test, and deploy software. It typically includes planning, requirements analysis, design, implementation, testing, deployment, maintenance phases. . 124

Supervisory Control and Data Acquisition A type of industrial control system used to monitor and control industrial processes and infrastructure.. 28, 124

supply chain A network of organizations, people, activities, information, and resources involved in a organisations process. 4–6, 14, 21–28, 126