TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Sander Eesmaa 204793 IVCM

SUPPLY CHAIN INFORMATION SECURITY MANAGEMENT IN ESTONIAN ORGANIZATIONS

Master's thesis

Supervisor: Kristjan Karmo
MBA

Tallinn 2023

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Sander Eesmaa 204793 IVCM

TARNEAHELA INFOTURBE JUHTIMINE EESTI ORGANISATSIOONIDES

Magistritöö

Juhendaja: Kristjan Karmo
MBA

Tallinn 2023

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Sander Eesmaa

15.05.2023

Abstract

Supply chain has been increasingly targeted in the cyber domain. By recognizing the potential risks associated with information security in the supply chain, organizations can take a proactive approach to managing their cyber security measures. This involves extending their focus beyond their own internal cyber security measures and implementing information security controls across their supply chain.

The study employs mixed-method approach to assess the level of awareness and implementation of supply chain information security management best practices among Estonian companies, and qualitative approach has been employed to analyse the open-ended responses and derive insights about participants' expectations, preferences, and experiences.

The outcomes show the importance and level of supply chain information security controls implementation and, develops functional requirements and user stories to be the starting point of the development of supply chain information security management tool.

This thesis is written in English and is 88 pages long, including 6 chapters, 10 figures and 13 tables.

Annotatsioon

Tarneahela infoturbe juhtimine Eesti organisatsioonides

Tarneahel on üha enam küberrünnakute sihtmärgiks. Tarneahelas infoturbega seotud võimalikke riske teadvustades saavad organisatsioonid oma küberturvalisuse meetmete haldamisel ennetavalt läheneda. See hõlmab nende keskendumist oma sisemistest küberkaitse meetmetest kaugemale ja infoturbe rakendamist kogu tarneahelas.

Uuringus on kasutatud hübriidanalüüsi, et hinnata tarneahela infoturbe juhtimise parimate tavade teadlikkuse taset ja rakendamist Eesti ettevõtete seas. Samuti rakendati kvalitatiivset lähenemist, et analüüsida avatud vastuseid ja saada ülevaade osalejate ootustest, eelistustest, ja kogemustest.

Tulemused näitavad tarneahela infoturbe kontrollide rakendamise olulisust ja taset ning loodi funktsionaalsed nõuded ja kasutajalood, mis on tarneahela infoturbe juhtimise tööriista arendamise sisendiks.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 88 leheküljel, 6 peatükki, 10 joonist, 13 tabelit.

List of abbreviations and terms

2FA	Two-factor authentication
CIS	Centre for Internet Security
CISO	Chief Information Security Officer
CRO	Chief Risk Officer
CTO	Chief Technology Officer
HIPAA	Health Insurance Portability and Accountability Act
ICT	Information communication technology
ISMS	Information security management system
ISO	International Organization for Standardization
LLC	Limited Liability Company
MFA	Multifactor authentication
NIST	National Institute of Standards and Technology
OSINT	Open-source intelligence
PCI DSS	Payment Card Industry Data Security Standard
PII	Personally identifiable information
SBOM	Software bill of materials
SC	Supply Chain
UI	User interface
US	United States

Table of contents

List of figures

List of tables

1 Introduction

1.1 Motivation

In the 1st quarter of 2020, the world saw one of the biggest supply chain cyber incidents in history so far. The widely known SolarWinds cyber attack targeted US federal government, state and local governments, and the private sector in US. Threat actors embedded malicious code in the SolarWinds's Orion software, and this was unknowingly distributed by SolarWinds to their clients via a software update. [1]

This is only one example of cyber attacks against supply chain in recent history. It is, unfortunately, a perfect example how supply chain can be effectively exploited to conduct cyber attacks. Threat actors are finding different ways to their targets and use any means and take any paths necessary to achieve their goal. By targeting supply chains, the threat actors are able to compromise many targets via a single point of entry. Or on the other hand, can compromise a target with hard to penetrate information security posture by using the target's supply chain as an enabler.

By recognizing the potential risks associated with information security in the supply chain, organizations can take a proactive approach to managing their cyber security measures. This involves extending their focus beyond their own internal cyber security measures and implementing auditing and compliance checks throughout their supply chain. Such checks can be facilitated by a supporting tool, such as a software solution designed to help organizations manage their supply chain information security. By utilizing such a tool, organizations can more effectively identify and address potential vulnerabilities in their supply chain and ensure that all parties involved in the supply chain are adhering to the necessary information security standards and protocols.

1.2 Problem statement

The primary goal of this study is to identify the problems and shortcomings of supply chain information security management, identify the awareness level and gaps. Additionally, the study aims to identify the functional requirements and user stories for a tool that could help key stakeholders to manage their supply chain information security posture. The result for this should be a comprehensive set of requirements and user stories that can be used as a starting point for developing a software tool to support supply chain information security management.

The author proposes following research questions:

1. To what extent are Estonian companies aware of and implementing supply chain information security management best practices?

2. What are the specific functional requirements and user stories Estonian companies expect from ICT tools for supply chain information security management?

The outcome of the study will be a literature research of the current mindsets of threats and benefits of supply chain information security management. Also, to demonstrate the importance of supply chain information security management. Additionally, based on the outcome of market analysis a theoretical development plan for a tool will be recommended to help manage supply chain information security. However, due to the main focus of the study being on the perspective of cybersecurity, the proposed input for the development of the tool will be limited to identifying functional requirements and creating user stories. It is important to note that the development of such a tool is beyond the scope of this study due to the extensive time, financial, and human resources required. Therefore, the primary aim is to propose a theoretical development plan that can guide future study and development in this area.

1.3 Novelty

The present study analyses the existing literature on the subject to prove the problem of maintaining information security in the supply chain. Past academic research has often taken an analytical approach. The focus of this study is slightly different. It seeks to establish a foundation for a tool development. The tool is intended to manage information

security compliance in the supply chain. To achieve this, functional requirements and user stories for such a tool are analysed. This would directly contribute to improving the supply chain information security management.

The work is novel as the cybersecurity landscape for Estonian organizations has previously not been researched from the perspective of supply chain information security management.

2 Literature review

Linton et al. [2] acknowledge the benefits of information technology in supply chain but point out that there are also unanticipated consequences to it. The openness and accessibility that it brings to supply chain also create the need for security. The need for security reflects the more general challenge of living in a more open and integrated world economy. The core issue is how to manage the risk in this environment not exclusively in cyber supply chain but in information technology and innovation management in general also. Article highlights that there is much to research on this topic, develop understanding of the challenges, solutions, and theory.
Korolova [3] describes supply chain attack when an attacker infiltrates the organisations systems through a third-party partner or provider who has access to your systems and data. The partner in the supply chain can be anyone who produces any kind of software or hardware. In general, it can be anyone in your supply chain who has access to your systems and/or data.

Smith et al. (2007) researched the nature of information security risk in the supply chain management and analysed the findings of a conducted survey. As a result, supply chain information security risks were mapped where it shows how risks originate from either organization, network or environmental sources and how certain processes and links are vulnerable to IT threats. With this it is shown that supply chain is affected by IT threats, thus supply chain information security risks are to be included in the general supply chain management. [4]

Colicchia et al. [5] discuss research areas on information sharing in supply chains and risks that are related to them. They bring out the current status and shed light to the future. Their article is based on Systematic Literature Network Analysis method. For example, in their literature review they found out that there is a lot of information about the current status of information sharing in the supply chains, but future predictions are lacking. It is an issue because there probably will be a lot of turbulent changes in the area. Also, they found that literature regarding the topic is lacking an external IT and security perspective,

meaning viruses, hackers, etc and found out that literature is focusing more on internal threats. Furthermore, they say that complexity of supply chains might also become an enormous issue regarding potential risks to the information in the supply chain.

Nasir et al. (2015) find that cyber security, being part of information security, is one of the main issues in the global supply chain. One of the important things is to identify and analyse the cyber security vulnerabilities to enable correct countermeasure to mitigate the threats. From the perspective of the energy sector, it has been researched that these aspects can have an impact on the reputation and overall confidence amongst stakeholders which in return can result in financial losses. To counter this with a modular approach, as researched in the global oil supply chain, the potential cyber threats at every step and corresponding countermeasures are identified. Thus, it is critical to assess and analyse cyber threats at every step in the supply chain due to its ripple effect because if they are properly identified they can be suitably dealt with. [6]

Urciuoli and Hintsa [7] are bringing out that one of the problems for supply chain is the cybersecurity and lack of it can lead to different crimes. Also, partner's trust and verification, physical assets management gaps, reverse flows or human resources are also risks that can lead to crimes. The study points out the importance of security awareness and risk management in the supply chain. Information technology systems should be the enablers of supply chain and not vectors that can be exploited to attack and impact those systems security. Fortunately, supply chain owners mostly acknowledge the importance of the topic, and they are increasing the security of their IT systems, otherwise systems will be just the most vulnerable part of the supply chain.

In June 2010 one of the most famous cyber attacks took place which targeted the Iranian nuclear facility and was named "Stuxnet". It was essentially a computer worm with the level of sophistication and technical characteristics that had not been seen in the world so far. Farwell et al. (2011) analysis focuses on the characteristics and operation of the malware. It was a targeted malware aimed against the Iranian nuclear program. It targeted specific frequency-converter drives and altered the frequency of the electrical current that powers the nuclear centrifuges. Through that the cyber attack manipulated with Iran's nuclear program by sabotaging the normal operation of the process.[8]

This showcases a very extreme case of how IT threats and cyber attacks might affect an organisation through its supply chain. The attack did not target the IT assets of Iranian nuclear plant but instead affected the plant through third-party software and systems – in this case the target was Siemens SCADA system.

In December 2013 another example of supply chain attack took place in the U.S against Target. Threat actors had stolen 40 million Target credit and debit card records by accessing point of sales systems. The attack lifecycle included a step where the threat actors targeted a company in Target's supply chain, Fazio Mechanical, to send them an e-mail with malicious attachment several months prior the data breach. Through that the threat actors were able to compromise Fazio Mechanical systems and gained access to it. This in turn was leverage to access Target's systems through a vendor portal which in the end granted access to the Target's systems for the attackers to exploit further. In this supply chain attack case, from the perspective of cyber supply chain risk management, Target could have implemented compliance requirements against vendors such as require implementation of proper malware defences, cyber security awareness training requirement for the staff and multifactor authentication amongst many others.[9]

Next year, after the Target incident, in 2014, Home Depot supply chain attack took place [10] where similarly to Target the point of sales systems were compromised. Like in Target incident in this supply chain attack the attackers managed to gain access to Home Depot point of sales systems through a third-party vendor logon credentials. Total of 56 million credit and debit card information was stolen. Besides other more general information security countermeasures that could have stopped the attack there are also supply chain specific countermeasures that they did not apply – supply chain vendor identity and access management. Auditing the vendors is key aspect and could have helped stopping both Target and Home Depot supply chain attacks. The two attacks are very similar which shows how supply chain security is most often than not on the important controls list, otherwise Home Depot could have protected itself against such attacks from the Target breach happened a year before.

A more recent example of supply chain attack is from 2020 [11] and is known as the SolarWinds attack. Attackers gained access to the source code for the SolarWinds Orion monitoring and management software. By inserting malware in the software's source code and by SolarWinds distributing this given update to their clients the affected systems

were all compromised and gave the attackers control and access over them. Affected clients included thousands of organisations over the world. Amongst others many U.S government entities. Again, by attacking one target in a supply chain the threat actors are able to compromise numerous organisations. SolarWinds trusted position in different organisation's supply chains made it the perfect target for a supply-chain attack. A report [1] concludes that the SolarWinds supply chain attack shows the importance for security to be considered as part of the vendor selection lifecycle. The supply chain attacks do not only target hardware and software vendors but anyone who has access to your systems or data in any way or form.

McFadden and Arnold find in their article that the extent of supply chain problems have not been strictly defined and thus appropriate defences not developed. They focus on the aspect how important government organizations use variety of third-party software and hardware as part of their supply chain which can enable the attacker to compromise the given organizations. Due to the sensitive nature of for example Department of Defence they see inspection and testing at the receiving end of the distribution phase as one of the solutions in the supply chain risk management. They have focused on acceptance testing as one of the key controls of supply chain information security risk. [12]

Nadya Bartol describes in her article how supply chain management has developed. Many standards and best practices of supply chain management has been developed and over time they have been refined. Through community reviews, where practitioners from different communities have had to collaborate in a joint effort, the standards and best practices have been updated and can thus be used across multiple professional domains. One of the most known set of standards are from the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), Centre for Internet Security (CIS) Critical Security Controls, and The Open Group. Each of them trying to adapt and refine the set of rules to be acceptable to all participants.[13]

For example, NIST has integrated recommendations for supply chain risk management into several of their guidance's like the Cybersecurity Framework, Risk Management Framework, and Security and Privacy Controls for Information Systems and Organizations (SP 800-53R5) [14]. Such standards and best practices provided

organisations essential frameworks to build their supply chain risk management and compliance checks up on.

Technology Innovation Management Review publication [15] takes a more precise turn on the matter of supply chain management and handling the subject of cyber-risk and cyber-resilience in supply chain management. It is proposed that in order to start successfully managing organisation's supply chain one should take following actions:

1. Map the supply chain.
2. Build capability.
3. Share information and expertise.
4. State standards and best practices across your supply chain
5. Measure, assess, audit.

All this is in support of managing the supply chain risks in a manner that prepares and enables organisations to return to business as usual after an incident has occurred or to be able to mitigate an incident in the first place.

Boyson (2014) talks about cyber supply chain risk management as a sub-branch of the general supply chain risk management with the focus on helping IT executives taking on the globalization of supply chain parts like hardware and software. S. Boyson has conducted a survey and an analysis on this field. The goal was to develop organisational assessment tool and a capability/maturity model with focus on this sub-branch of supply chain risk management. The result of this research is the developed maturity model that which acts as an assessment tool for organisation to identifying itself in the cyber supply chain risk management domain. It also encourages similar tools to emerge in the future through further research. The key factors in cyber supply chain identified were governance, systems integration security and operations security. [16]

An exploratory analysis is conducted by Colicchia et al. [17] that how organisations approach and to what extent in the cyber supply chain risk management. A qualitative approach based on a comparative case study analyses five large companies. The key findings show that in addition to having information security policies and checks in place

internally it is also becoming more and more a requirement to extend the security mindset to one's supply chain and adopt concepts like prepare, respond, recover, and maintain.

Simon and Omar [18] analyse the challenge of cybersecurity in supply chain and view how coordinated and uncoordinated investments in cyber security can have different effects. They also applied another dimension to the view of the attacker being strategical or non-strategical but the overall key findings here are that investment coordination in cyber security in the supply chain is critical.

Keskin et al. [19] also emphasize the importance of strengthening the security of organisations supply chain. In their study they compare and present exploratory analysis of the different methods for managing cyber supply chain risk management that are developed by different entities with main goal of discovering the common indicator and criteria of such assessments. The key findings show that although several analysed entities have their own means of assessing and scoring a given organisation in regards of cyber supply chain risk, they all do it from their own perspective. This calls for a more standardized approach to the topic.

Ponemon Institute LLC conducted a study about the challenges organisations face when they attempt to protect the data shared with their supply chain. The findings show the increase of risk of sharing confidential and sensitive data with third parties is increasing. As a countermeasure in the supply chain risk management there are governances and best practices that can be used to reduce the risk of a data breach through the supply chain. The general effectiveness of supply chain governance and best practices remain low based on the survey participants. They also report that more than half of the respondents lack the overview of who they share sensitive data in their supply chain. Additionally, if an evaluation is conducted against the supply chain it most of the times culminates with signatures on a contract and no real assessment is conducted. [20]

Ghadge et al. [21] study focuses on investigating cyber supply chain risk management by conducting descriptive and thematic analysis. The key outcomes were development of a

conceptual model (Figure 1) that shows strong link between information technology, organisation, and supply chain security systems.

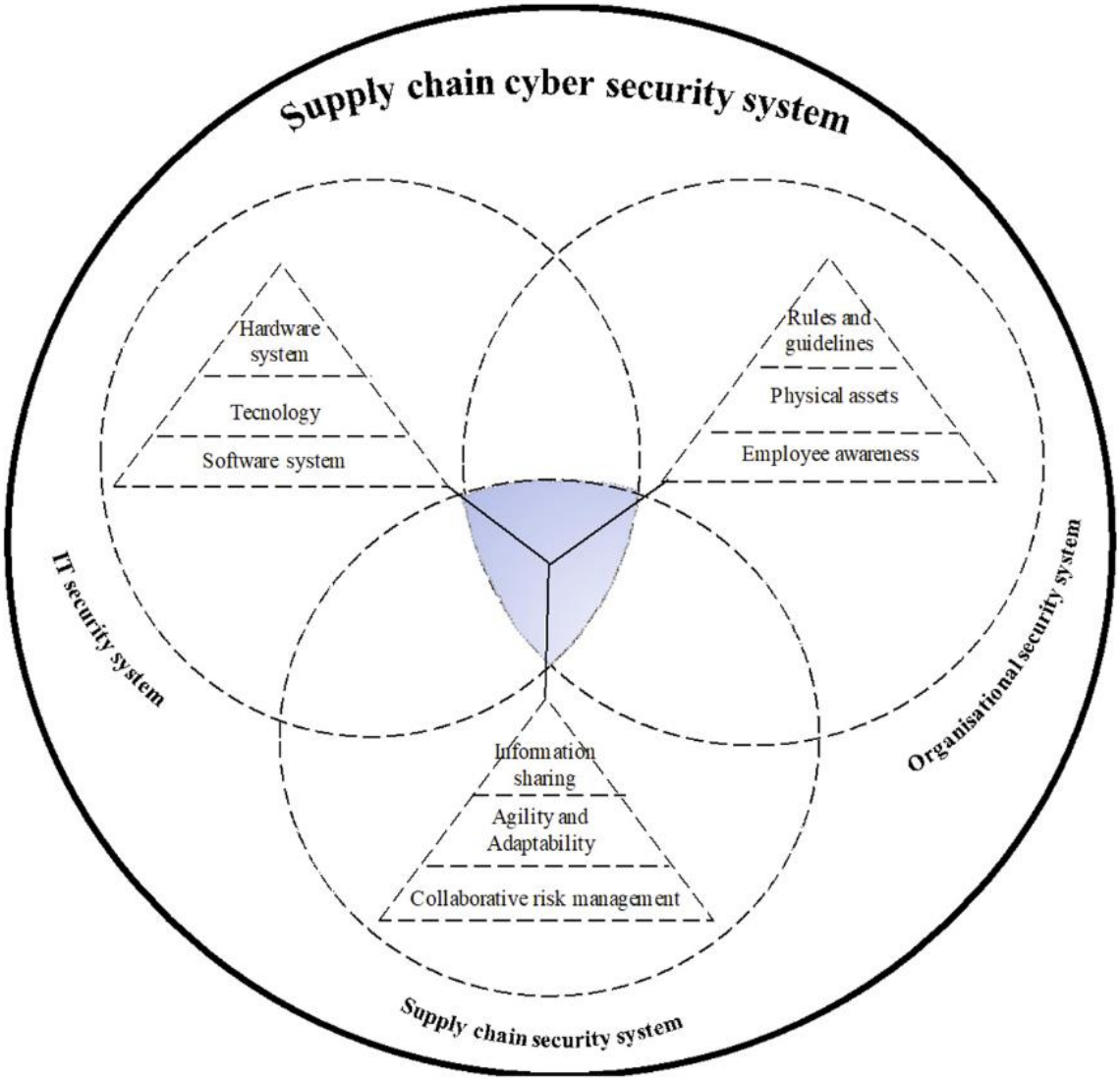

Figure 1. A conceptual model for supply chain cyber security system [21]

Additionally, although human aspects of cyber security are critical, the technical aspect still attracts more attention. Creating supply chain cyber-resilience requires more effort in raising awareness, standardizing policies and best practices and creating collaborative strategies and empirical models. [21]

Research paper from Faisal et al. [22] identifies various information risks that can impact a supply chain and a conceptual framework is developed to quantify and mitigate the identified risks. The framework aims to guide supply chain and IT managers in

understanding and managing the corresponding risks. Faisal et al. identified twelve variables that could support in the process of supply chain risk management.

Enablers	1	2	3	4	5	6	7	8	9	10	11	12	Driver
1. Information sharing	1	1	0	1	1	0	1	1	0	1	1	1	9
2. Supply chain wide strategies	0	1	0	0	1	0	0	0	0	1	1	1	5
3. Level of supply chain integration	1	1	1	1	1	1	1	1	1	1	1	1	12
4. Collaborative relationships	1	1	0	1	1	0	1	1	0	1	1	1	9
5. Support to partners	0	0	0	0	1	0	0	0	0	1	0	1	3
6. Reliable IT/IS infrastructure	1	1	1	1	1	1	1	1	1	1	1	1	12
7. Top management commitment	0	1	0	0	1	0	1	0	0	1	1	1	6
8. Trust among partners	1	1	0	1	1	0	1	1	0	1	1	1	9
9. Awareness about information risks	1	1	1	1	1	1	1	1	1	1	1	1	12
10. Availability of funds	0	0	0	0	1	0	0	0	0	1	0	1	3
11. Incentives alignment	0	1	0	0	1	0	0	0	0	1	1	1	5
12. Metrics for assessment and analysis	0	0	0	0	0	0	0	0	0	0	0	1	1
Dependence	6	9	3	6	11	3	8	6	3	11	9	12	

Table 1. Enablers for supply chain risk management [22]

Variables like awareness about information risks, reliable infrastructure and level of supply chain integration have strong driver power and less dependency. Therefore, these are strong drivers and identified as the key enablers. It is suggested to take care these on priority basis since there are a few other dependent variables being affected by them. [22]

Davis [23] brings out different ways in his article how to use an information-centric approach and how to create more cyber-resilient supply chain in organization where information is shared in multiple supply chains. This is important to learn because so far physical aspects of the supply chain have been more important than protecting the information that it holds. Also, he provides five different steps that could be followed in order to protect its information better. Overall, it can be said that acquiring organization has few things they need to take into account in order to extend their cyber-resilience. Firstly, they need to map the supply chain. It could be difficult due to number of suppliers in organization or the eagerness of suppliers to concede their suppliers. Although, if organization succeeds to map their supply chain, they can be more prepared for potential incidents or interruptions and can be aware of the flaws of the supply chain. Second important thing that Davis brings out is building capability meaning that acquirers and supplier have to work together in order to create the secure environment for information. Other aspects that tie in with the previous one is sharing expertise and information - meaning if there are any threats, attacks, or incidents this information should be shared

and not kept to themselves because sharing information helps to find the weaknesses of the created system and improve its flaws. Fourth point is following state requirements across the supply chain and making sure that common standards, frameworks, and languages are used. Lastly, it is important that all organizations in supply chain measure, assess and audit their cyber-resilience.

Keegan [24] focuses on the insurance industry concerns that they have due to of using international technology supply chain and the article also brings out how coordinated approach can be provided by the international community. It is important to find ways how to secure the supply chain globally because by not doing that it may cause huge severance in the world's economics. For example, government could be a big supporter here. Although, they have mainly been focusing on defending the military and on protecting intelligence, they now see that private networks also need security. There are different examples of the United States, Russia, India or China where government has helped to improve domestic IT industry and infrastructure. Keegan says that in order to create more secure cyber environment countries should focus on a National Cyber Security Strategy and developing, re-evaluating and maintaining it. Clear cyber security strategy should be set and government, industry, etc. should be involved in order to enhance the effectiveness of the measures. Collaboration with other countries is also needed and understanding that secure cyberspace should be constantly developed.

A conceptual view on information security in supply chain by Sindhuja et al. (2015) researches the topic from a management controls perspective. The study analyses the need for a higher level of control over the existing controls in the inter-organisational context. Authors also point out that instead of seeing information security in supply chain as a cost it should be taken as an essential part of the supply chain process in the light of the business environment becoming more of a collaboration among organisations rather than a competition. It is also seen that the level on information security awareness inside an organisation is well-recognized, but the inter-organisational context is yet to see more attention due to most supply chains involving multi-organisational and trans-border relationships. [25]

Putrus [26] in his ISACA journal article reviews the risk-based management approach to supply chain data security, risk, and compliance. Supply chain partner or third parties, as

stated in the article, can be anyone who provides services in any way or form to an organisation and all of them are subject to be assessed regarding the risks they might impose. The article suggests the development of a third-party risk register to provide standardized way for an organisation to evaluate and quantify the severity and exposure of risks sourced from the supply chain vendors. With this implemented, the organisation can dictate type and frequency of compliance reports requested from those vendors.
Firstly, inventory of potential vendors should be compiled. Then create a risk register by mapping the risks of selected vendors. Thirdly, determine documents and evidence that shall be requested from the vendors to showcase their compliance or non-compliance with any relevant information security standards e.g. Next, each vendor's risk should be assessed and aggregated which concludes the vendors being classified and place in the appropriate risk category. The last step of the model is ongoing monitoring, reviewing, and reporting of the analysed risks.

Survey conducted by Creazza et al. [27] analyses the level on perception of cyber supply chain risk management in over 100 Italian organisations. It shows an overall acknowledgment of the significance of the topic. The participants find it is essential to secure the data shared in the supply chain. The overall alignment of perceptions is found but this might differ in some items by the respondents' groups like manufacturers, logistics, retailers. The study also indicates that human factor is found to be most important source of risk in the cyber supply chain. While the general awareness of the importance of countermeasures is high the level of perception again differs by group. To compare, retailers have a weaker perception than logistics. As one of the directions for future research the study sees the investigation of technologies and tools that can improve the cyber supply chain risk management process.

Bandyopadhyay et al. [28] study the incentives to invest in information security among supply chain partners. The operational benefits of collaboration among supply chain are significant and well known but this also increases the information security risk in the supply chain. It is found that to manage supply chain effectively and in collaboration the partners should include mechanisms that will support the organisations to focus on the other partners information security and not only on their own. Organisations that are part of a given supply chain have more incentive to invest into information security when a

liability mechanism is implemented for example. This induces the partners to invest at the social optimal level.

Pandey et al. [29] are focusing on cyber security risks in global supply chains in their article. Authors have found 16 cyber security risks that are grouped in three categories: supply, operational and demand risk. Amongst others, they also propose that information security standards, specifically NIST framework, are key elements to support managing cyber security risks in the supply chain. Also, the article brought out few different cyber-attack methods that are used against supply chain management systems. Methods are as follows: password sniffing and cracking software, spoofing attacks, denial of service attacks, direct attack, malicious tampering, and the insider threat. Which in turn shed light in the value of applying relevant information security requirements across the supply chain.

2.1 Research gap

The primary research gap resides in that most academic research focuses on analytical point of view or proposing standards or models at most. Rather than solely analysing the information security aspects of the supply chain, current research is geared towards establishing a foundation for the development of a tool that can manage information security compliance in the supply chain. This approach would have a direct impact on enhancing the overall management of supply chain information security.

In [13] and [14] a more standardized approach is taken for supply chain information security management. While the standards might be widely accepted and used, they are still inconvenient to apply in the supply chain. This still calls for a technological means or a tool that supports the management of the risks while also following the standards and best practices.

McFadden's and Arnold's [12] study proposes practical way of tackling supply chain information security risk and suggest implementing the process of testing whether an item is compromised or not. Although implementing an ADHOC-based countermeasure is a practical solution, it primarily focuses on addressing specific incidents and may not effectively manage risks in general. To supplement this approach, auditing and assessment measures for supply chain partners should be incorporated alongside of

hardware testing. This thesis aims to achieve this goal by proposing a framework that enables the auditing and assessment of supply chain partners to manage risks more effectively. By implementing this, organizations can have a comprehensive view of the risks associated with their supply chain partners and take proactive measures to mitigate them.

3 Methodology

The study employs mixed-method approach combining both quantitative and qualitative research methods. For quantitative research a questionnaire with Likert scale questions and general questions was created. The goal was to assess the level of awareness and implementation of ISO27001-based supply chain information security management practices among Estonian companies. This approach allows to analyse the numerical data collected from the questionnaire to draw conclusions and identify awareness and gaps. In the study a 4-point Likert scale is used and the scale ranges from “strongly disagree” to “strongly agree”. Due to the small size of Estonian market and that each company can only present one answer a 4-point scale was chosen. This forced participants to represent their opinion and left out the option to answer neutral.

Additionally, through opinionated questions we have identified the functional requirements and user-stories for ICT tools supporting supply chain information security management based on the questionnaire answers. This shows that qualitative approach has been employed to analyse the open-ended responses and derive insights about participants' expectations, preferences, and experiences.

Before distributing the questionnaire, a target list of 84 Estonian companies was compiled. All companies were unique so that each answer can represent one company. The persons receiving the questionnaire were picked out based on their role in a given company. More specifically the focus was on roles and positions that highly likely deal with the challenges of supply chain information security or are responsible for this subject. Those are for example chief information security officers, chief technology officers, chief risk officers, cyber security experts, cyber security department managers, etc.

Out of the 84 companies approached for the study, 30 responded to the questionnaire which makes the response rate 35,7%. Out of the 30 respondents 4 were not Estonian companies (Australia 3, Gibraltar 1). While this study focuses on Estonian companies the 4 answers were disregarded making the final sample size 26 Estonian companies.

The study's questionnaire utilized in this study is based on ISO27001 and its corresponding standard, ISO27002, which outlines specific controls to be followed. To ensure the validity of the formulated questions, the CIS Critical Security Controls were also used to support the questionnaire's design. By incorporating these two widely accepted information security standards, the formulated questions are validated and adhere to industry best practices. This approach enhances the reliability and validity of the research findings, thereby increasing the robustness of the research methodology.

International Organization for Standardization (ISO) is a worldwide organization where members interested in a subject can participate in a technical committee created to develop a certain international standard. Amongst others ISO has created a collection of Information Security Management system family of standards. It consists of many different editions but most notably in the scope of current academic study ISO27000, ISO27001 and ISO27002. ISO27000 provides an overview of the ISMS family of standards and additionally introduction to ISMS and the related vocabulary. ISO27001 is a more specific standard and provides requirements to develop and operate an ISMS including how to maintain information security in supply chains. ISO27002 complements ISO27001 by defining specific control objectives and best practice controls when implementing requirements from ISO27001. [30]

Regarding Supplier Relationships information security, ISO27001 A.15.1 Information security in supplier relationships specifically sets out three controls. There are shown in Table 2. The objective of these is to ensure the protection of organization assets that partners in the supply chain have access to. [31]

A.15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.
A.15.1.2	Addressing security within supplier agreements	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or

		provide IT infrastructure components for, the organization's information.
A.15.1.3	Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

Table 2. ISO27001 A.15.1 Information security in supplier relationships [31]

Furthermore, ISO27002, expands ISO27001 with a list of controls that can be applied while implementing ISO27001. Each control (A.15.1.1-A15.1.3) have a list of specific guidelines that can be chosen to follow to achieve compliance with ISO27001. ISO27002 A.15.1 guidelines are listed in Appendix 2 – ISO27002 15.1 Information security in supplier relationships guidelines [32]. [32]

Centre for Internet Security (CIS) is a community driven non-profit that is, amongst others, responsible for CIS Critical Security Controls. It is a collection of actionable controls that defenders can use. The controls are derived from real-world cyber attacks and threats that are collectively put together by experts that represent every role and sector in the field. Each control identified to be included in this critical list includes a set of safeguards of the topic and is given a description and explanation of its importance. More specifically CIS Critical Security Control number 15 "Service Provider Management", shown in Table 3. It describes the need to evaluate service providers and to ensure that they protect the systems and data appropriately. This control describes how organizations rely more and more on their supply chain for managing data or infrastructure for applications, functions, or other services. Moreover, there are numerous examples of incidents out in the wild that prove this. For example, how payment cards are compromised by an attacker infiltrating a vendor in retail industry. Or how enterprises have been affected by disruption to business due to a third-party service provider being hit by a ransomware attack in their supply chain. It is found that there is no universal standard for assessing security in the supply chain. This means that many service providers are being audited by their customers with custom made checklists more often than not. These are usually carried out and managed through spreadsheets. This process

ends up affecting the service providers own business. The control (CIS Critical Security Control number 15) states that regardless of the organizations size there should always be a policy on how to review service providers in the supply chain. All service providers should be inventoried and have a risk rating about their potential impact to the business in the case of an incident. Supply chain should be assessed and the adherence to expected security level should be monitored. On top of all that there should always exist a contractual agreement regarding security requirements. Those should at least include minimum information security requirements, incident notification and response and points of contact. [33]

Nr.	Safeguard description
15.1	Establish and Maintain an Inventory of Service Providers
15.2	Establish and Maintain a Service Provider Management Policy
15.3	Classify Service Providers
15.4	Ensure Service Provider Contracts Include Security Requirements
15.5	Assess Service Providers
15.6	Monitor Service Providers
15.7	Securely Decommission Service Providers

Table 3. CIS Critical Security Control number 15 safeguards

3.1 Ethics

In this study, ethical considerations were prioritized to protect the privacy and confidentiality of the participants. An anonymous questionnaire was utilized, ensuring that no personally identifiable information (PII) was requested or collected throughout the survey process. By not collecting any PII, the study minimized the risk of disclosing personal data or violate the privacy of the respondents. This approach ensures that all responses remain anonymous, making it impossible to link individual answers to the identities of the participants. In line with ethical research practices, participants were also informed about the study's purpose, the voluntary nature of their participation, and the

confidentiality measures in place. Thereby promoting transparency and creating trust between the researcher and the respondents.

3.2 Limitations

Several limitations were identified in this study. First, some participants expressed unwillingness to disclose sensitive information related to their company's supply chain information security practices. This was expected due to the participants working in cyber security area in one way or another, which might make them more careful of who and what information they share.

Second, related to the cyber security domain again, some participants replied that they don't open links from strangers. Again, this can be expected since phishing is one of the most used attack vectors amongst cyber criminals.

Third, one respondent gave feedback that the questionnaire was too lengthy, which may have contributed to survey fatigue and reduced the response rate.

Fourth, when analysing the answers, it was realized that the study's 4-point Likert scale has an inherent limitation when differentiating between "disagree" and "strongly disagree". For example, when asked if inventory of suppliers is established and maintained, it logically doesn't matter if the respondent answers "disagree" and "strongly disagree".

Fifth, the structure of the questionnaire contained some errors which revealed only after the questionnaire was already distributed and some answers already collected. Repetitive questions about ICT tools led to inconsistent or incomplete responses. Respondents that already provided quality answers in previous questions tended to provide less meaningful answers for the last ICT tools related questions.

Lastly, the sample size of 26 Estonian companies may not be sufficiently representative to make broad conclusions about supply chain information security management practices.

A limitation, that doesn't affect the outcome of the analysis of the results is the inclusion of organization size categories (1-9, 10-49, 50-249, 250-1500, and more than 2000) in the questionnaire. This may have limitations in terms of its alignment with the Estonian

standard size categories. It is important to note that in this study, the results of organization sizes are not modified but they are recategorized to correspond with the main classes:

- micro enterprises: less than 10 persons employed;
- small enterprises: 10-49 persons employed;
- medium-sized enterprises: 50-249 persons employed;
- small and medium sized enterprises (SMEs): 1-249 persons employed;
- large enterprises: 250 or more persons employed.

4 Results

The sample size for this study consisted of 30 companies from various industries and sectors, with the majority of responses (26) coming from companies based in Estonia (Figure 2). The sample includes diverse range of perspectives on the topic of information security in the supply chain in Estonia. It is important to note that the 4 companies not based in Estonia will not be included in the study, as the focus is specifically on Estonian organizations. While the sample size in this study may seem relatively small it is important to consider the niche focus of this study and also the additional limitations pointed out in paragraph 3.2. On the other hand, to ensure high-quality and relevant data IT, information security professionals and people responsible for supply chain information security were specifically targeted. This allowed to gain insights from individuals who are directly responsible for managing information security in the company's supply chain. It is noteworthy that all of the respondents held positions related to IT or information security, which enhances confidence in the quality and relevance of their answers. Surprisingly, 73% of the respondents held the position of Chief Information Security Officer (CISO), while the remaining respondents were either IT managers, held similar roles or were on the management board (Figure 3).

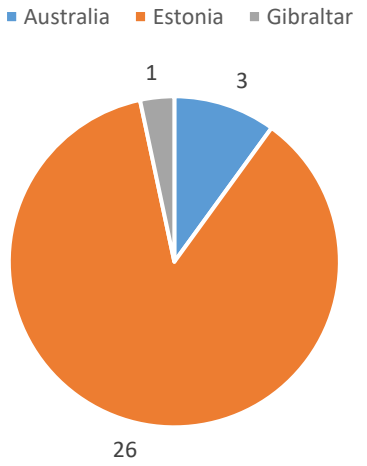

Figure 2. Country of operations

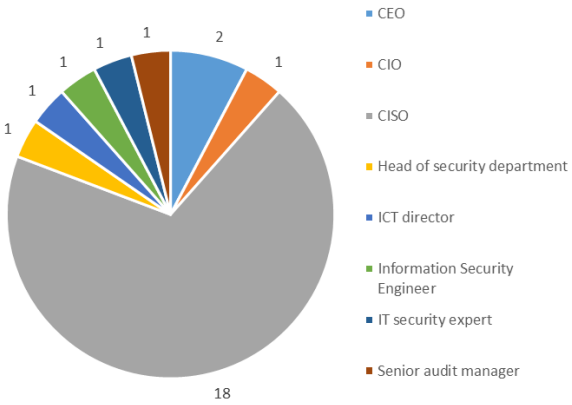

Figure 3. Titles/positions

The field of operation can significantly influence a company's approach to managing information security in the supply chain. Our study analysed the remaining sample size of 26 companies, representing a diverse range of fields. These include cyber security, education, energy, financial services, gaming, government, healthcare, human resources, identity management, information technology, IT audit/consulting, logistics, public sector, security, and telcos (Figure 4). The broad range of fields included in our sample enabled a more comprehensive cross-market analysis. This provides valuable insights into the unique challenges and opportunities for information security in the supply chain across different sectors.

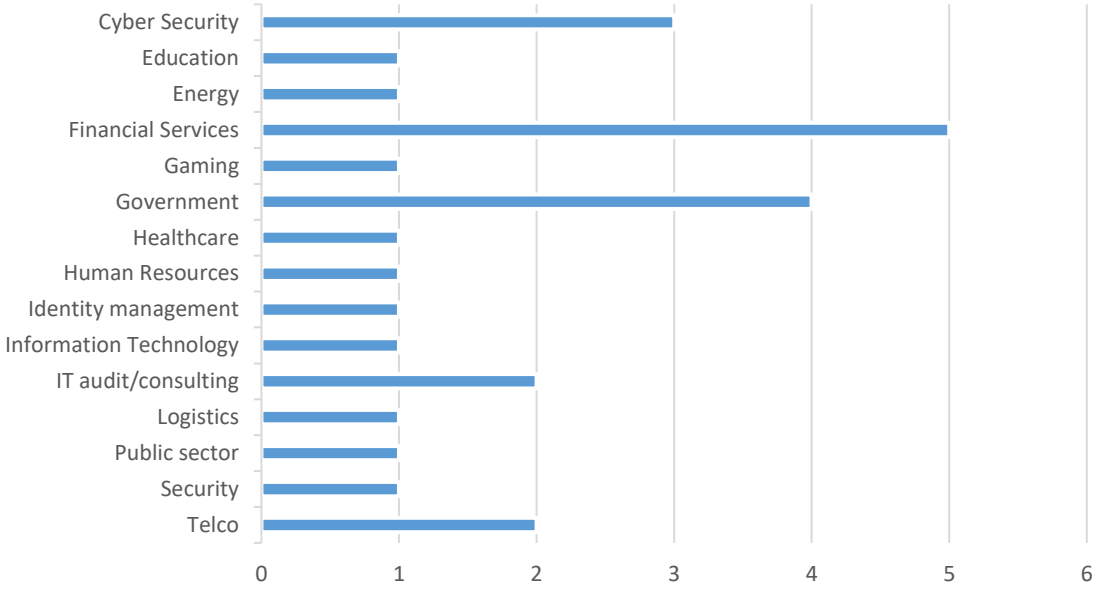

Figure 4. Field of operation / business area

Adding to that, all of the organization sizes recognized in Estonia [34] are represented in the sample size of 26 companies including micro, small, medium and large enterprises (Figure 5). The inclusion of all organization sizes in the sample adds a valuable level of variety and confidence to this study. It allows us to explore how supply chain cyber security practices may differ across organizations of different sizes, and to identify common challenges and best practices that are relevant for companies operating in different size categories.

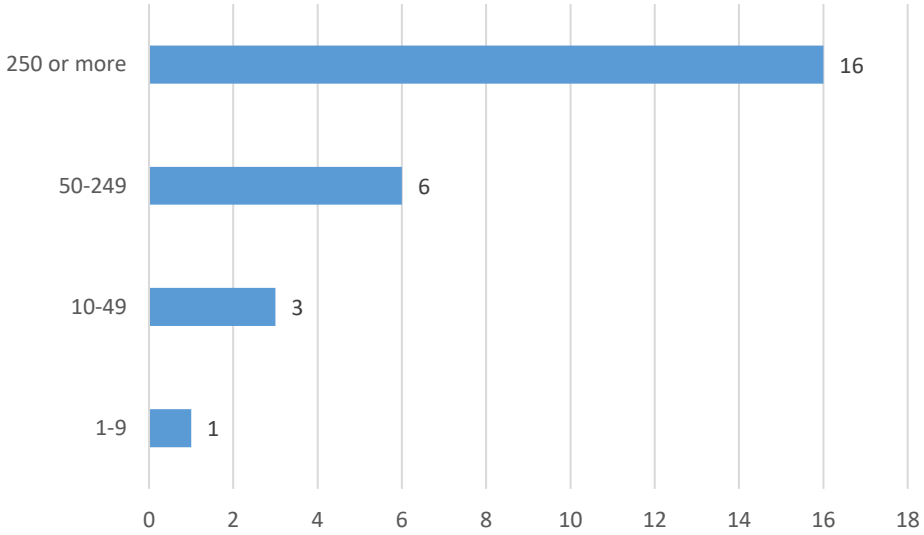

Figure 5. Organization sizes

Out of the 26 companies sampled, it appears that the majority do not own any recognized information security certification. Total of 16 respondents said that they have not obtained any certificates. Although, out of those 16 two companies said that they are planning to obtain a certification and another two said that they are in the progress of obtaining a certification. The low number of companies that have obtained certification may be cause for concern. It suggests that many companies in the sample may not have adequate measures in place to protect their information and may be vulnerable to potential security breaches. Additionally, the fact that only a small number of companies are in the process of obtaining certification or have plans to do so may indicate a lack of awareness about the importance of information security certification or a lack of resources to pursue certification.

Although the majority of the companies, 16, in the sample do not own an information security certificate a significant minority have done so (Figure 6). The remaining 10 companies that said they do own an information security certificate make 38% of the sample size. This is quite significant if we also consider how difficult a certification process can be and that not all compliant companies towards some standards seek certification for it. Although the latter is likely a rather rare occasion.

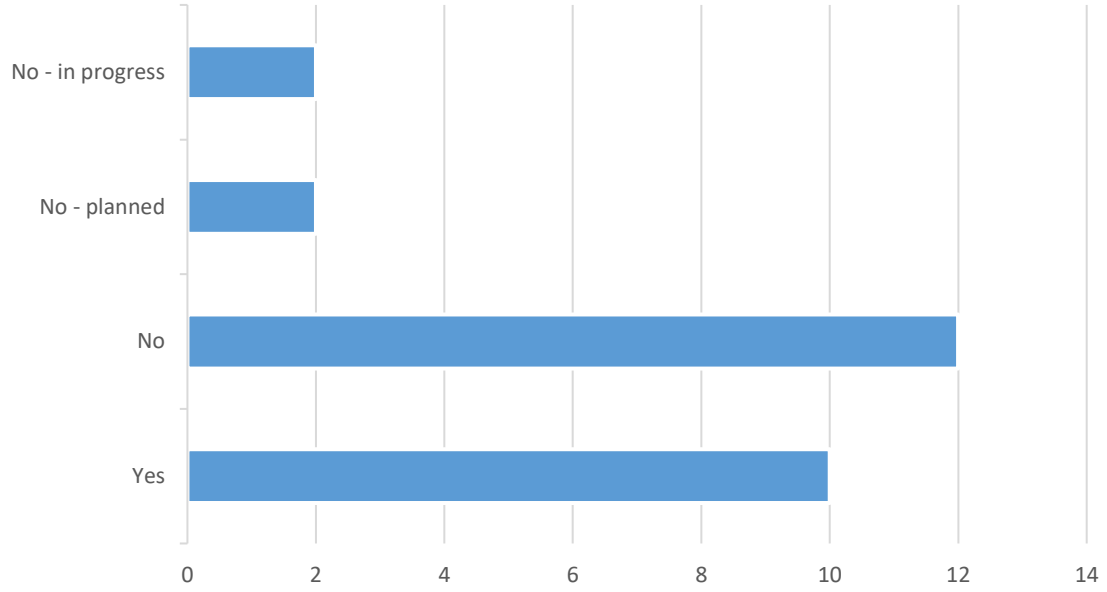

Figure 6. Does the organization hold any information security certificates?

Based on the responses of the 26 companies sampled, there appears to be no noticeable correlation between company size and whether a company holds information security certificates. Even among the large companies with 250 or more employees, some reported not having certificates, while the majority of the medium sized companies reported having certificates. Similarly, companies that reported having certificates, were planning or in-progress to get certificated, were distributed across a range of company sizes, including 10-49, 50-249 and 250 or more employees [34].

This finding suggests that the decision to pursue information security certification may not be driven solely by company size or resources. Other factors such as the type of information the company handles, regulatory requirements, client and supply chain

partners demands may play a more significant role in driving the decision to pursue certification.

An important finding to note is that among the 14 companies holding or seeking information security certificates, the majority have opted for ISO27001 certification. These companies either already hold the certificate, are in the process of obtaining it, or have future plans to secure it. One of the respondent's answers didn't clarify which certificate their company owns. Besides ISO27001, the respondents also mentioned the Estonian Information Security Baseline, Estonian Information Security Standard, SOC 2 Type 2, and Payment Card Industry Data Security Standard (PCI DSS) certificates.

4.1 Supplier management process and information access

Based on the responses of the 26 participants in this study, it appears that the majority of organizations have a process in place for managing suppliers. Specifically, 16 participants agreed with the statement "The organization has a process in place for managing suppliers," while 8 participants strongly agreed with the statement. This indicates that based on the assessment of the respondent their company has done very well in establishing supplier management process.

When asked about supplier information access the responses show a lot lower level of confidence on how well given companies do it. This is a critical aspect of information security in the supply chain, as it helps to protect the confidentiality, integrity, and availability of information. Although the majority of companies (24) are controlling and monitoring information access, only 4 of them indicated that this has been done very well in their company.

Only 2 participants disagreed with both statements.

4.2 Inventory of suppliers

Out of the sample size of 26 there were 22 companies that agreed or strongly agreed with the statement “Inventory of suppliers is established and maintained”. While only 4 thought that they are doing it very well there is major change when asking about the importance of keeping such inventory. It appears that there is a significant level of agreement regarding the importance of establishing and maintaining an inventory of suppliers. 20 respondents answered with strongly agree which makes 77% of the sampled organizations. This suggests that organizations recognize the importance of having an inventory of suppliers and view it as a key component of supply chain information security management. While 2 participants answered that they agree that keeping and maintaining inventory of suppliers is important it doesn’t affect the significant majority thinking of it as a critical element.

Additionally, the 22 companies that have a supplier inventory established, generally see this task rather difficult. While being an important control in supply chain information security 12 companies find it difficult and 7 find it very difficult. Only 3 companies see

that supplier inventory is not that difficult to build and maintain and have disagreed with the statement “Supplier inventory is complex to build and maintain”.

The feedback from the remaining four respondents, who do not maintain a supplier inventory, is enlightening. Their responses suggest a discrepancy between the perceived importance of keeping a supplier inventory and the actual implementation of this practice. It seems that the theoretical value of this procedure does not necessarily translate into consistent application. While inventory of suppliers isn’t kept, all of the companies see it as important or very important thing to do. This suggests that there may be barriers or challenges preventing these companies from implementing supplier inventory management practices. A notable point of contention is that all four companies recognize the importance of maintaining a supplier inventory, yet they do not practice it. Interestingly, two of these companies believe that building and maintaining a supplier inventory is not complex at all. This contradiction highlights the gap between perception and implementation in these organizations. This can’t be explained without further research and deeper dive into specific company’s policies and practices.

4.3 Information security assessment

The results of the questionnaire suggest that assessing the information security level of suppliers is an important aspect of supply chain information security management. With 19 participants agreeing and 3 participants strongly agreeing with the statement "Supplier's information security level is assessed". The findings show that organizations are aware of the potential risks associated with supplier information security vulnerabilities and are taking steps to mitigate them through supplier assessments.

Furthermore, the majority of participants, 15 of whom strongly agreed and 7 who agreed, believe that it is important to evaluate suppliers’ information security level. This underscores the importance of information security in the supply chain. Also, it shows the need to prioritize the assessment of supplier information security levels as a part of managing the risk in supply chain information security.

There are still unknown challenges that companies face that this study is unable to specify. Specifically, despite four companies reporting that they do not assess the information security level of their suppliers, they all still view it as an important control to implement.

Adding to it, 2 of those companies don’t think it is complex at all to evaluate supplier information security level.

Additionally, the sample size of 26 were also asked whether they collect evidence to verify the information security level of their supplier. Out of the 22 that said to assess their supply chain information security levels, only 9 said to collect evidence to verify the assessment and just 2 strongly agreed with the statement showing that they think their company is doing it very well. Remaining 11 companies assess their suppliers but face challenges in collecting evidence to support their assessments. The difficulty of collecting evidence to support supplier information security assessments is a significant obstacle that many companies face. It requires careful planning, execution, security and trust between the supplier and the company to ensure that the information gathered is both relevant and reliable. Also, supplier information security assessments can be complex and time-consuming, which may further contribute to the difficulty of collecting evidence to support these assessments.

4.4 Minimum information security requirements

The survey participants were asked whether their organizations had minimum information security requirements in place for their supply chain partners. Out of the 23 that do set such requirements only 5 strongly agreed with the statement “Minimum information security requirements and controls are set for suppliers”. This indicates that there is room for improvement in most of the sample companies. With one exception, these companies regarded this control as important with the majority leaning towards very important with answering strongly agree to the statement. Interestingly, one company that claimed to be implementing this control very well and find it as a very complex task, controversially doesn’t see this control to be important.

The responses indicate difference of views regarding the statement “It is complex to define and set such requirements and controls”. While 7 companies found this control to be easy to implement, the majority of the sample regarded it as a complex task, with five describing it as "very complex".

Out of the sample size of 26 the 3 companies that do not have minimum information security requirements and controls set for suppliers all still considered this task to be

important. They all also agree that it is complex to define and set such requirements. One of the companies differed from the other two. They said to be documenting and signing the minimum information security requirements in an agreement that is signed by all parties. This again is a controversial finding but cannot be further explored with the current approach and answers.

Overall, the majority of respondents reported that they include information security requirements in a signed agreement, with only 7 answering “no” to the question. Of these seven, 5 organizations had the requirements and controls set but didn’t include them in a signed agreement. Thus, the general approach is positive since additionally to setting the requirements and controls it is essential to have them clearly documented and agreed upon by all parties involved.

4.5 Adherence to information security requirements

While it is important to set minimum information security requirements and controls in the supply chain it is as important to monitor the adherence to them. Agreements can hold anything you put into them and there is a chance companies agree with terms they haven’t even read through. When asked whether adherence to minimum information security requirements and controls is monitored 15 of the 26 companies answered “disagree”. This is a significant risk that the companies accept. Furthermore, if no other risk mitigation methods are not used, then companies solely rely on the given agreement that their partner adhere to the minimum information security requirements and controls. Although, all of the 15 say that it is either important or very important to monitor such adherence there is still something holding them back from doing it. One of the reasons is complexity of monitoring the adherence. Out of the 15 that do not monitor adherence to minimum information security requirements admit that it is either a complex or very complex task. Only 2 didn’t agree that it is a complex task. This shows controversy when seeing it as an easy task but not implementing this risk mitigation method.

As those 15 companies don’t monitor the adherence to the requirements the majority expectedly answered that they don’t collect evidence to verify the adherence to those requirements. Two companies stand out by saying that they are collecting evidence while answering that they don’t monitor the adherence. This is likely an error or other specific

characteristics of those companies that the scope of this academic study questionnaire cannot explore.

The remaining 11 companies of the sample size of 26 said that they are monitoring adherence to minimum information security requirements and controls. Two of those companies say that they do it very well. All of the companies see it as an important task with 7 of them saying it is very important. With one exception they all also find it a complex task. When asked whether they collect evidence to verify the adherence to information security requirements 5 companies disagreed with the statement. From the other 6 that collect evidence two say that they are doing it very well.

Overall, while monitoring adherence to minimum information requirements and controls is a complex task by itself the companies additionally seem to struggle with collecting evidence to verify the adherence. Across the whole sample 18 companies answered that they are not doing it and only 8 do.

4.6 Incoming compliance requests

Thus far, the study has primarily focused on obtaining information regarding supply chain information security management specifics of participating companies. However, the sample of 26 companies were also asked whether they themselves receive requests to be compliant with certain set of information security requirements by their partners. Given the increasing attention that supply chain information security is receiving from companies, the responses provide valuable insights. With 18 out of the 26 respondents indicating that they receive such requests on a regular basis. Specifically, one company reported receiving daily request, 8 companies monthly, 5 companies quarterly and 4 companies yearly. These findings suggests that significant workload is put into dealing with the requests. When asked how long it usually takes to put together an answer per request the most popular answer was 3-4 hours followed by 5-6 hours. However, three companies reported that it might even take up to weeks. Notably, out of the 18 companies that receive information security compliance requests, 11 are also required to provide evidence to verify the compliance. The remaining companies don’t have to provide evidence.

4.7 Use of ICT tools across all statements

The sample size of 26 were asked whether they use any sort of ICT tools to support supply chain information security management. The participants shared insights across the domains addressed in this questionnaire – inventory of suppliers, information security assessment, adherence to minimum information security requirements and incoming compliance requests. Additionally, they were able to describe what they would change about the tool and asked to provide opinion on what would they expect most from such ICT tools generally. These answers will be one of the core inputs for describing a supply chain information security management software functional requirements.

4.7.1 ICT tools for establishing and maintaining supplier inventory

To keep and maintain inventory of suppliers 15 companies said to be using some form of ICT tool. Controversially, out of the 11 that don't use ICT tools for it, 8 companies have answered that they keep inventory of suppliers and think it as an important and complex task. One of the possible reasons for this situation might be that not all respondents acknowledged that in the context of this question even the simplest tool like an e-mail or spreadsheet software is considered an ICT tool. Amongst the 15 companies that use ICT tools, Microsoft 365 product family or other spreadsheet type of tools were mentioned the most. The main benefit being that while being basic, these kinds of tools are simple to use and have a low learning curve. On the other hand, being too basic was brought out as a drawback amongst lack of automation, suiting only simple processes and lack of integration options. Overview of all the tools with benefits and drawbacks brought out by the respondents are shown in table Table 4 (page 43-44). Only a few of the companies brought out what they would change about the tool they use:

- Integrate it to pipeline.
- Add data regarding suppliers' certificates, ICT systems.
- Consolidate and integrate the tools.
- Dedicated supplier management platform.
- Fire some people responsible for supplier management.

With one exception, these can be helpful to better determine functional requirements for a new tool.

ICT Tool	**Benefits**	**Drawbacks**
MS365 (e-mail, excel)	Not much, easy to use.	No automation or central management.
Jira and different ERP solutions	Keeping track of contracts and inventory	Fragmentation. There are too many tools.
For contractual parties contracts register plus some other tools. For open-source part self-built tools based on opensource scanners.	In software development is important to have and manage SBOM (Software Bill of Materials).	Reactive (not proactive).
Internal registry	There is a registry.	Focus on business, not security.
It is in place, but I don`t remember the name.	Overview, including for example information about different issues and incidents (if there are any) with the supplier, supplier audit results (if we have done one) with gap mitigation plan overview.	I get the information I need (at the moment) from it.
Document management system through contracts	None really.	Not meant for supplier inventory management.
MS office	Simple	Too basic, manual.
Monday.com	Visibility and ease of use	Manual work

Through contract management	Nothing to point out. It is meant for contract management.	It is meant for contract management. Doesn't offer much for supplier inventory.
Email, MS office, ticketing system	Generally good and easy to use, low learning curve.	Lacks functionality, automation.
Google Sheets	Flexible.	Only fits a simple process and low number of suppliers.
Spreadsheets	Analytics, cloud service.	Lack of integration.
N/A	Usability, automatization.	In-house development.
Webware Webdesktop	Highly configurable.	Outdated interface.
Snipe-IT	Free, community support, regular updates, user-friendly UI.	In the case of multi-site, users cannot see the petty cash issued to them.

Table 4. ICT tools used for establishing and maintaining inventory of suppliers.

Expectations for an ICT tool that would support establishing and maintaining inventory of supplier's responses ranged in detail significantly. From simple as "ease of use" to detailed descriptions like "inventory, risk assessment, and support for other internal processes (budgeting, reuse, etc)". All the responses are shown in table below (Table 5, page 45-46) and will be later used to develop functional requirements. The data has been modified to improve grammar and translate one answer to English that was given in Estonian.

1. Easily manage and overview suppliers.
2. Automation of tasks, centralized management, history, overview, reports.
3. Better visibility and ability to stop builds.
4. Inventory, risk assessment, and support for other internal processes (budgeting, reuse, etc).
5. In case of a cyber incident to quickly get information regarding who is involved and what might the impact (including spill over).
6. Having an overview in detail about the suppliers (including history).
7. All-in-one. Keep track of contracts, licenses, inventory, and ticketing. Also, to have OSINT information about the partners/suppliers.
8. Link to Procurement process.
9. Automation of tasks, centralized management, history.
10. Easy to use UI. Overview of partners and their compliance to minimum infosec requirements.
11. Usability
12. User friendly UI.
13. Easy data management.
14. Supplier inventory and management. Ease of use to create questionnaires and store information.
15. User friendliness.
16. Easy to use and give good overview.
17. Visibility, control, time saving.
18. Validity of contract, supplier contacts and representatives, supplier accesses to internal systems etc.
19. The tool should make management easier.
20. Ability to perform auditing on top of the information shared.
21. Access management, security auditing.
22. Easily and centrally managed supplier inventory system.
23. Ease of use.

24. Excel table.

25. All the information about suppliers should be in one place and you should be able to manage them in the same place too.

26. Ease of use and security (2FA etc), accessibility (cloud), ensured data integrity (encrypted backups for example).

Table 5. Expectations for supplier inventory tool

4.7.2 ICT tools to assess supplier's information security level

While 22 companies, a significant majority (85%), said to be assessing supplier's information security level, less than half of them use an ICT tool to do it. Overview of the feedback is shown in Table 6.

ICT Tool	Benefits	Drawbacks
Office	Simple to use	Not made for the job
3rd party certificates or audits	Get some information	Depends on 3rd party and often the audit is on another scope
Security Scorecard	It gives some OSINT about the partner/supplier	It gives only a score about the perimeter services of the supplier.
MS office	Simple	Too basic
MS365	Not much, easy to use.	No automation or central management
Word and Excel based questions.	Not much. Just enables to format questions and make it sort of easy to fill for partners.	Just a text-based approach. Nothing is automated or centrally managed.
Vulnerability scanners, OSINT tools. Not specific tools that measure security level, but rather tools that give us some sort of insight of the situation.	We can assess what is the security posture from outside.	Limited visibility on internal procedures and controls.
Email, MS Office	Simplicity	Lack of security and functionality. Too basic and heaps of manual work.
A questionnaire	None really	Provides false sense of security and risk management
Same as before	Same as before	Same as before

Table 6. ICT tools to assess supplier's information security level.

Out of the 11 company's answers 8 also provided optional feedback on what they would change if they could. With three exceptions these are again important input for formulating functional requirements based on end-user's input:

- Define the scope of the audit.
- Would like to have more OSINT in-depth information about supplier.
- More automation
- See previous.

- Assessing security level needs to take into account all aspects of the enabled controls and established procedures.
- I would bring onboard a system that is easy to use but secure and automated.
- Fire some people, as above.
- Same as before

There was good quality of answers across the sample size of 26 about the expectations for a tool that should support assessing supplier's information security level. Only three of the companies provided no meaningful answer – "N/A" and "same as before". The data is brought out in Table 7 below.

1. Biggest supply chain attack is not from contractual parties! That cannot be evaluated by any tools. For contractual ones would be nice to see compliance against some standard (NIS, ISO27001)
2. Automated supplier risk assessment
3. Easy to use.
4. Central place for all information
5. N/A
6. Easy to use and good overview.
7. Visibility, control, time saving.
8. Compliance certificate, compliance and security score given by well-known service providers (e.g., Azure, Palo Alto etc.)
9. It should make the evaluation process easier.
10. Compliance to standards
11. Ease of use
12. To evaluate suppliers' information security level you basically need an auditing tool.
13. Excel table
14. All info in the same place. Automation, simple to use workflows.
15. Enough coverage to provide an accurate overview of their security posture.
16. Comprehensive and easy to use assessment for both parties.
17. Audit should be honest.
18. Quick report about possible partner/supplier

19. Automation of tasks, centralized management, history 20. Easy to use UI. Overview of partners and their compliance to minimum infosec requirements. 21. Supplier inventory and management. Ease of use to create questionnaires and store information. 22. Ease of use so this could be adopted by organizations that have limited technical knowledge. 23. Automation, simplicity 24. Highlight suppliers and issues that would require human intervention - assessment, decisions, negotiations etc. 25. Same as before 26. N/A

Table 7. Expectations for a tool to assess supplier's information security level.

4.7.3 ICT tools to monitor adherence to information security requirements

Monitoring adherence to minimum information security requirements is a complex task. As described in paragraph 4.5 Adherence to information security requirements on page 40 the majority doesn't monitor it. Thus, as expected, very few of the companies use an ICT tool to support it. Four companies did provide answers about what they use but the quality of the answers was very low and won't support describing functional requirements much, as seen in Table 8.

ICT Tool	**Benefits**	**Drawbacks**
MS365	see previous	see previous
same as before	same as before	same as before
MS office like above said. Annually ask to renew the answers to the questionnaire.	Not much. Just enables to format questions and make it sort of easy to fill for partners.	Same as above
N/A	N/A	N/A

Table 8. ICT tools to monitor adherence to minimum information security requirements.

There is a bit more detail in then answers when the companies were asked about the general expectation for a tool to support monitoring adherence to minimum information security requirements. Nonetheless, there are 7 answers that provide no further support in developing functional requirements.

4.7.4 ICT tools to handle incoming information security compliance requests

The sample of 26 were not exactly asked to describe what ICT tools they use to handle incoming information security compliance requests. Instead, the companies were asked if they have received such requests and how do they map and track these requests. Surprisingly, out of the 18 answers many provided meaningful input about the tool the companies use for mapping and tracking the requests (Table 9).

How do you map and track these requests?
1. It's dedicated team's responsibility to track these requests.
2. Contracts department deals with these requests.
3. Excel
4. In email
5. Audits mostly
6. Excel
7. Manually
8. Not at the moment
9. Dedicated tool + Excel
10. Mostly ISO27001 certificate is asked.
11. E-mail
12. Digital documentation system mostly
13. E-mail, MS office
14. Not very well
15. See previous.
16. Document management system

17. Manually through e-mail and files.
18. Document management software

Table 9. Overview how respondents map and track incoming information security compliance requests.

5 Developing functional requirements and user stories

The study aims to identify the functional requirements and user stories for a tool that could help key stakeholders to manage their supply chain information security posture. The result for this will be a comprehensive set of functional requirements and user stories. These can be used as a starting point for developing a software tool to support supply chain information security management. The functional requirements will be based on information security standard and end-user feedback and will lay the groundwork for creating user stories based on those functional requirements.

5.1 Functional requirements

Through open-ended questions we have identified what benefits and drawbacks respondents see in ICT tools they use. Also, what they would expect from ICT tool supporting information security in supply chain. Based on these responses it is possible to generate functional requirements. This will be done from two perspectives. Firstly, from the perspective of ISO27001 information security standard. This incorporates widely accepted and acknowledged set of controls into the creation of functional requirements for supply chain information security management tool. Secondly, the input from the respondents, representing the needs of the market and end-user, is used to develop additional functional requirements.

5.1.1 Functional requirements from ISO27001

ISO27001 standard was partially used to create this study's questionnaire. It is widely accepted and acknowledge standard and provides requirements to develop and operate an ISMS including how to maintain information security in supply chains. Thus, it is also used to create functional requirements for a tool that could help key stakeholders to manage their supply chain information security posture. For this, more specifically the controls for information security in supplier relationships from ISO27002 Annex 15.1 (Appendix 2 – ISO27002 15.1 Information security in supplier relationships guidelines [32]) are used. ISO27002 is often referenced when implementing ISO27001 requirements.

The specific controls are chosen based on the author judgment. All the controls are reviewed and phrased into a functional requirement where possible and meaningful. Overview of the chosen controls and the phrased functional requirement is shown in Table 10 below.

ISO27002 Annex A.15.1 control [32]	Phrased functional requirement
A.15.1.1. a	The software must enable users to categorize types of suppliers.
A.15.1.1. b	The software must allow users to manage the whole supplier lifecycle.
A.15.1.1.c	The software must provide overview of supplier accesses to information and systems.
A.15.1.1. d-e	The software must allow to define and monitor compliance to minimum information security requirements for each supplier.
A.15.1.1. f	The software must allow to include evidence that verifies the adherence to minimum information security requirements.
A.15.1.1. h	The software must provide overview of the incidents associated with each supplier.
A.15.1.1. l	The software must allow to link agreements associated with each supplier.
A.15.1.2. f	The software must allow to link and manage supplier contacts and representatives that will be allowed access to organization's systems or data.
A.15.1.2. j	The software must allow to categorize supplier as sub-contractors and link/unlink them to existing supplier relationships.

Table 10. Functional requirements derived from ISO27002 Annex A.15.1

5.1.2 Functional requirements from end-users

The sample of 26 companies were asked about ICT tools used across the domains of supplier inventory, information security level assessment and adherence, and handling incoming information security compliance checks. They provided feedback on which ICT tools they are using, the benefits and drawbacks of that tool, and what would they change

about the tool given the chance. Additionally, they were requested to describe what would be expected from a tool supporting the corresponding topic – supplier inventory, information security level assessment and adherence, and handling incoming information security compliance checks. Overview of this is described in paragraph 4.7 and the data gathered will be the source from where functional requirements will be phrased (Table 11). This will provide significant value to the supply chain information security management tool functional requirements through reflecting market opinions and needs into the requirements.

If an organization input translates into an already created functional requirement it will not be described again. This will exclude the possibility for duplicates and will in turn make the mapping of functional requirements significantly transparent.

ID	Functional requirement
Inventory1	The software must provide automation where possible.
Inventory2	The software must allow central supplier management – including contracts and inventory.
Inventory3	The software must enable proactive approach to supply chain information security management.
Inventory4	The software must offer overview from both business (e.g., agreements) and information security aspects (e.g., adherence to requirements).
Inventory5	The software must provide overview of issues and incidents associated with each supplier.
Inventory6	The software must enable to ingest supplier audits and corresponding mitigation plans where applicable.
Inventory7	The software must offer a cloud and on-prem based solutions.
Inventory8	The software must withstand management of extensive number of suppliers.
Inventory9	The software must support integration with other systems.
Inventory10	The software must keep an archive and provide users access to historical data.
Inventory11	The software must use OSINT to enrich the information about the supplier’s information security maturity level.

Inventory12	The software must provide overview of supplier compliance to minimum information security requirements.
Inventory13	The software must allow users to build, send, receive, and manage information security questionnaires.
Inventory14	The software must allow managing supplier contacts and representatives.
Inventory15	The software must provide overview of supplier accesses to organization's internal systems.
Inventory16	The software must have the option to perform auditing operations of the information gathered from suppliers.
Inventory17	The software must follow information security best practices (e.g., MFA, encryption) by being compliant to applicable information security standards (e.g., ISO27001).
Assessment1	The software must allow assessing suppliers based on selection of information security standards (e.g., ISO27001, NIST, HIPAA, PCI DSS, CIS Controls).
Assessment2	The software must display quick view of the supplier's information security maturity level value.
Assessment3	The software must allow acceptance of information security certificates which in turn will automatically make the given supplier compliant to a set of requirements.
Assessment4	The software must have the option to build automated workflows that must be flexible enough to fit different organization needs.
Assessment5	The software must also allow to accept incoming compliance checks and keep the lifecycle of those business flows too.
Assessment6	The software must allow generating quick report on suppliers.
Incoming1	In addition to supplier information security management, the software must also be able to store and manage the organization's information security level.

Table 11. Functional requirements generated from responses

One of the focuses of the study is on providing a comprehensive set of requirements and user stories. These can be used as a starting point for developing a software tool to support supply chain information security management. By not assigning priorities to the requirements and user stories, the paper can provide a complete and comprehensive view

of the features and functionality needed for the software tool without prioritizing one requirement over another. In addition, this can allow greater flexibility and adaptability in the development process.

5.2 User stories

User stories are a common method used in software development. They are descriptions of a potential use of a system based on the perspective of the users. [35]

The functional requirements described in paragraph 5.1 will be mapped to user stories. Mapping functional requirements to user stories helps to ensure that the development process is focused on meeting the needs and goals of the end-users, and that the software system is developed in a way that is consistent with the requirements and expectations of the stakeholders.

User stories are created on 28 unique functional requirements described based on ISO27001 Annex 15.1 controls and end-user feedback. In some instances, a functional requirement has been described from both the perspective of the information security standard and the end-user, resulting in duplication (Table 12). Still, it was important to describe both requirements initially to demonstrate that the requirement is significant in both perspectives – information security standard and end-user.

ID	Functional requirement
A.15.1.1. f	The software must allow to include evidence that verifies the adherence to minimum information security requirements.
Inventory5	The software must provide overview of issues and incidents associated with each supplier.
A.15.1.1.c	The software must provide overview of supplier accesses to information and systems.
Inventory15	The software must provide overview of supplier accesses to organization's internal systems.
A.15.1.1.d-e	The software must allow to define and monitor compliance to minimum information security requirements for each supplier.
Inventory12	The software must provide overview of supplier compliance to minimum information security requirements.

A.15.1.1. l	The software must allow to link agreements associated with each supplier.
Inventory2	The software must allow central supplier management – including contracts and inventory.
A.15.1.2. f	The software must allow to link and manage supplier contacts and representatives that will be allowed access to organization's systems or data.
Inventory14	The software must allow managing supplier contacts and representatives.

Table 12. Overview of duplicate functional requirements

Out of the 33 functional requirements described from information security standard and end-user feedback 28 unique requirements remained. These functional requirements will be mapped to user stories. List of remaining unique functional requirements:

1. The software must enable users to categorize types of suppliers.
2. The software must allow users to manage the whole supplier lifecycle.
3. The software must provide overview of supplier accesses to information and systems.
4. The software must allow to define and monitor compliance to minimum information security requirements for each supplier.
5. The software must allow to include evidence that verifies the adherence to minimum information security requirements.
6. The software must allow to link and manage supplier contacts and representatives that will be allowed access to organization's systems or data.
7. The software must allow to categorize supplier as sub-contractors and link/unlink them to existing supplier relationships.
8. The software must provide automation where possible.
9. The software must allow central supplier management – including contracts and inventory.
10. The software must enable proactive approach to supply chain information security management.
11. The software must offer overview from both business (e.g., agreements) and information security aspects (e.g., adherence to requirements).

12. The software must provide overview of issues and incidents associated with each supplier.
13. The software must enable to ingest supplier audits and corresponding mitigation plans where applicable.
14. The software must offer a cloud and on-prem based solutions.
15. The software must withstand management of extensive number of suppliers.
16. The software must support integration with other systems.
17. The software must keep an archive and provide users access to historical data.
18. The software must use OSINT to enrich the information about the supplier's information security maturity level.
19. The software must allow users to build, send, receive, and manage information security questionnaires.
20. The software must have the option to perform auditing operations of the information gathered from suppliers.
21. The software must follow information security best practices (e.g., MFA, encryption) by being compliant to applicable information security standards (e.g., ISO27001).
22. The software must allow assessing suppliers based on selection of information security standards (e.g., ISO27001, NIST, HIPAA, PCI DSS, CIS Controls).
23. The software must display quick view of the supplier's information security maturity level value.
24. The software must allow acceptance of information security certificates which in turn will automatically make the given supplier compliant to a set of requirements.
25. The software must have the option to build automated workflows that must be flexible enough to fit different organization needs.
26. The software must also allow to accept incoming compliance checks and keep the lifecycle of those business flows too.
27. The software must allow generating quick report on suppliers.
28. In addition to supplier information security management, the software must also be able to store and manage the organization's information security level.

To map these 28 functional requirements to user stories a widely used user story template of "As a [persona], I [want to], [so that]" is used. The main persona used for this is supply chain manager which can also be a CISO, CTO, CRO or any role in the organization that

is responsible to managing information security in the supply chain. “Want to” will describe the intent the persona has and “so that” will describe the overall benefit gained by doing the “want to”. [35] The user stories follow the numbering seen in the above list of functional requirements so that each user story can be easily mapped to a functional requirement.

User Story 1.1:
As a supply chain manager, I want to categorize suppliers by their types, so that I can better organize and manage them according to their roles and importance in the supply chain.

User Story 2.1:
As a supply chain manager, I want to manage suppliers through their entire lifecycle, from onboarding to termination, so that I can maintain a consistent and effective supply chain.

User Story 3.1:
As a supply chain manager, I want to view an overview of supplier accesses to information and systems, so that I can ensure appropriate access controls are in place and monitor any unauthorized access.

User Story 4.1:
As a supply chain manager, I want to define and monitor compliance to minimum information security requirements for each supplier, so that I can ensure they meet our organization's security standards.

User Story 5.1:
As a supply chain manager, I want to upload and attach evidence that verifies a supplier's adherence to minimum information security requirements, so that I can maintain a record of compliance.

User Story 6.1:
As a supply chain manager, I want to link and manage supplier contacts and representatives who are allowed access to our organization's systems or data, so that I can ensure proper access controls are in place and there are no unauthorized accesses.

User Story 7.1:
As a supply chain manager, I want to categorize suppliers as sub-contractors and link or unlink them to existing supplier relationships, so that I can manage the complexity of our supply chain and maintain visibility of all parties involved.

User Story 8.1:
As a supply chain manager, I want the software to automate tasks where possible, so that I can save time and reduce manual effort in managing information security in the supply chain.

User Story 9.1:
As a supply chain manager, I want a centralized system to manage suppliers, including contracts and inventory, so that I can efficiently track and maintain information in one place.

User Story 10.1:
As a supply chain manager, I want the software to enable a proactive approach to supply chain information security management, so that I can identify and address risks before they become critical issues.

User Story 11.1:
As a supply chain manager, I want an overview of both business and information security aspects for each supplier, so that I can make informed decisions and manage risks effectively.

User Story 12.1:
As a supply chain manager, I want to view an overview of issues and incidents associated with each supplier, so that I can analyse and address any risks or vulnerabilities in our supply chain.

User Story 13.1:
As a supply chain manager, I want to ingest supplier audits and corresponding mitigation plans to the system where applicable, so that I can track and manage compliance efforts effectively.

User Story 14.1:
As a supply chain manager, I want the software to offer both cloud and on-prem based solutions, so that I can choose the deployment model that best fits my organization's needs.

User Story 15.1:
As a supply chain manager, I want the software to withstand management of an extensive number of suppliers, so that I can scale my supply chain management efforts as needed.

User Story 16.1:
As a supply chain manager, I want the software to support integration with other systems, so that I can seamlessly connect it with existing tools and processes in my organization.

User Story 17.1:
As a supply chain manager, I want the software to keep an archive and provide users access to historical data, so that I can track and analyse changes over time.

User Story 18.1:
As a supply chain manager, I want the software to use OSINT to enrich the information about the supplier’s information security maturity level, so that I can make better informed decisions.

User Story 19.1:
As a supply chain manager, I want the software to allow me to build, send, receive, and manage information security questionnaires, so that I can effectively assess the security posture of my suppliers.

User Story 20.1:

As a supply chain manager, I want the software to have the option to perform auditing operations on the information gathered from suppliers, so that I can validate the accuracy and reliability of the data.

User Story 21.1:

As a supply chain manager, I want the software to follow information security best practices and be compliant with applicable information security standards, so that I can trust its security and integrity.

User Story 22.1:

As a supply chain manager, I want the software to allow me to assess suppliers based on a selection of information security standards, so that I can evaluate their compliance with various frameworks relevant to my organization.

User Story 23.1:

As a supply chain manager, I want to see a quick view of the supplier's information security maturity level value, so that I can easily assess their overall security posture.

User Story 24.1:

As a supply chain manager, I want the software to allow the acceptance of information security certificates, which will automatically make the given supplier compliant to a set of requirements, simplifying the compliance process.

User Story 25.1:

As a supply chain manager, I want the software to offer the option to build automated workflows that are flexible enough to fit different organizational needs, so that I can streamline supply chain management processes.

User Story 26.1:

As a supply chain manager, I want the software to accept incoming compliance checks and manage the lifecycle of those business flows, so that I can efficiently handle incoming information and maintain up-to-date records.

User Story 27.1:

As a supply chain manager, I want the software to generate quick reports on suppliers, so that I can easily share insights and make informed decisions.

User Story 28.1:

As a supply chain manager, I want the software to store and manage my organization's information security level in addition to supplier information security management, so that I can maintain a comprehensive view of our overall security posture.

6 Conclusion

Supply chain information security management importance is growing in time which is also show by this paper's literature review. A lot of research has been put into this subject and this study extends this by analysing Estonian market on this subject and providing recommendations for a practical solution.

Overview will be given based on the research questions stated at the beginning of this study.

Research question 1:

> To what extent are Estonian companies aware of and implementing supply chain information security management best practices?

Creazza et al. [27] say in their research that it has been found that majority of the market acknowledges the importance of supply chain information security management.

The analysis in this study shows that across all the controls that the questions were based on, companies express that it is extremely important to implement controls based on best practices. These controls include:

- inventory of suppliers;
- information security assessment;
- minimum information security requirements;
- adherence to minimum information security requirements.

Surprising 70% answered "strongly agree" to all such questions and 28% saying "agree" while only two questions about importance were answered with "disagree".

The implementation and complexity of doing it does not provide such positive outcome. Many companies don't have all the controls in place. The overall complexity of implementing the different controls appear to be rather high. Those two findings show that there are significant shortcomings in this that can be supported by a supply chain information security management tool.

On the other hand, there are many companies that said to be implementing many controls very well regardless of the complexity of the task. But this wasn't consistent across all the controls. While a company could be doing well in some of the controls they might be lacking in others. This again showcases the good level of awareness in the sample companies but lack of implementation.

Generalised overview is given in the table (Table 13) and figures (Figure 7, Figure 8, Figure 9) below. These visualise the results of this research in a simplified way. It is seen that across all the controls (inventory, assessment, minimum requirements, adherence) implementation of the controls is on a good level. While nearly all participants said across all the controls that the control is important to implement. Lastly, across all the controls, majority of participants answer that implementing the controls is a complex or very complex task.

	The control is implemented	The control is important	The control is complex to implement
Strongly disagree/Disagree	25%	2%	19%
Agree/Strongly agree	75%	98%	81%

Table 13. Summary of how participants agree/disagree across all controls

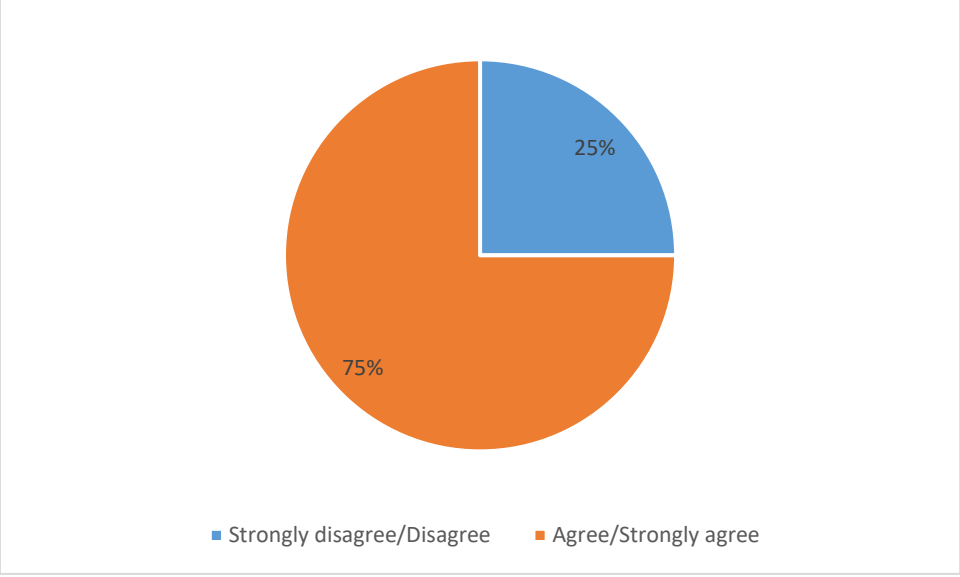

Figure 7. The control is implemented.

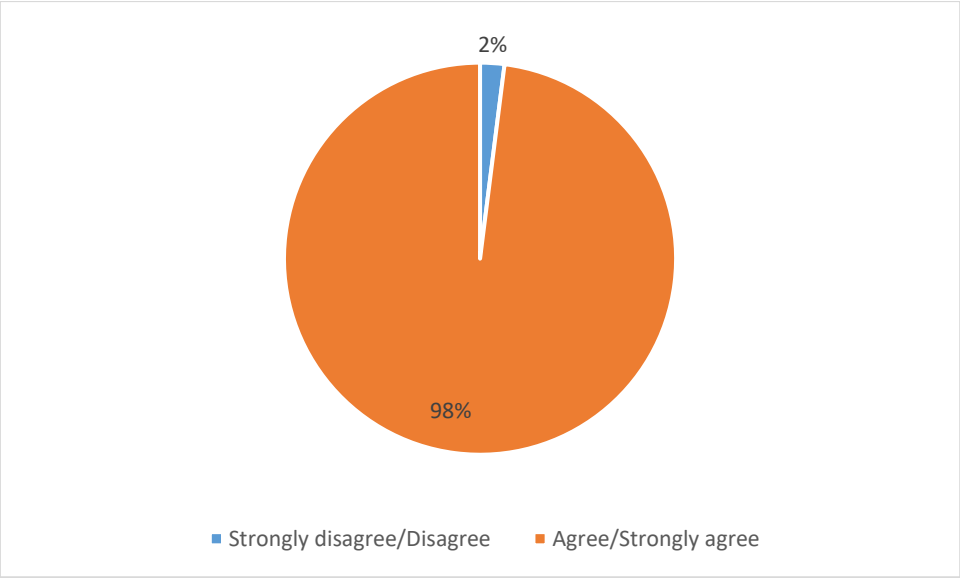

Figure 8. The control is important to implement.

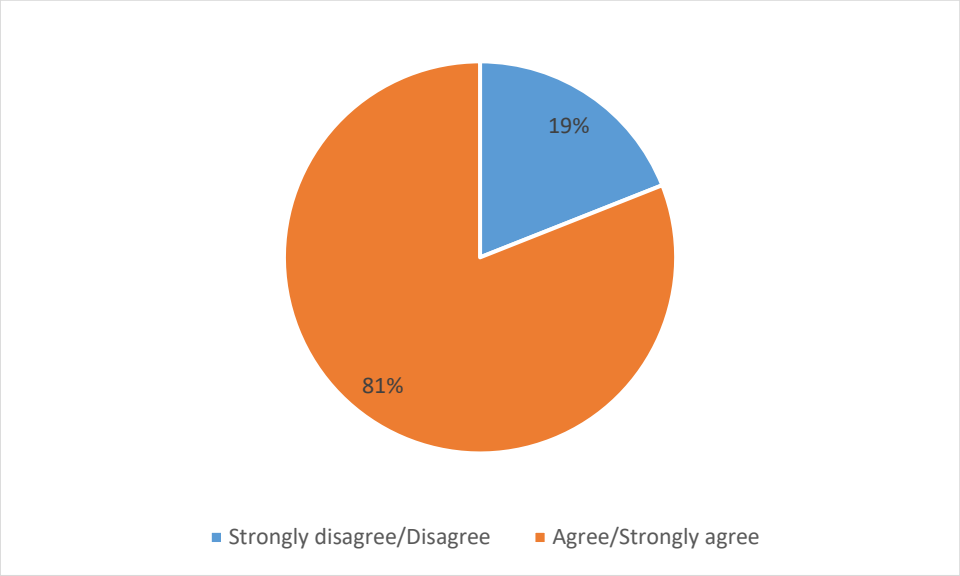

Figure 9. The control is complex to implement.

This overview clearly show that the sample of this research is clearly aware of the importance of supply chain information security controls. The sampled organizations could do better in implementing all the necessary supply chain information security controls but nevertheless 75% is a good level of implementation. The remaining controls that might not be implemented yet is certainly caused by the fact that majority of the controls are seen as complex or very complex to implement.

Research question 2:

> What are the specific functional requirements and user stories Estonian companies expect from ICT tools for supply chain information security management?

Creazza et al. [27] also found in their study that they see the investigation of technologies and tools that can improve the cyber supply chain risk management process an important subject to be researched.

Participating companies provided invaluable insight of benefits and drawbacks of the ICT tools they use and what would they most expect from a tool supporting supply chain information security management.

Functional requirements and user stories described in this paper provide a solid starting point on developing a supply chain information security management tool. With the 28 distinctive functional requirements and corresponding user stories the essential aspects and expectations of such tool have been effectively mapped. The development of the functional requirements and user stories was based on ISO27001 and end-user feedback, thereby ensuring that two crucial elements are integrated into the tool's design process. Overview of the mapped functional requirements and user stories can be found in Appendix 4 – Unique functional requirements and Appendix 5 – User stories, correspondingly. Those provide a comprehensive answer to research question number 2 and should be considered as core requirements for a supply chain information security tool.

It is important to note that the development of a tool was beyond the scope of this study due to the extensive time, financial, and human resources required. Therefore, the primary aim was to propose a theoretical development plan that can guide future research, work, and development on this topic.

6.1 Recommendations for further work

One of the limitations of the results is that it focuses on Estonian companies, future research could explore the topic in a more global context, comparing and contrasting the findings across different countries and industries. This would provide a broader perspective on supply chain information security management and identify unique challenges or best practices in different regions. Moreover, this approach will substantially enhance the quality of functional specifications and user stories and will enable representation of a broader range of regional markets. After exploring more large-scale markets and researching the mindsets of different countries and industries, more comprehensive functional requirements can be developed. It is likely that the functional requirements and user stories developed in this research will cover even worldwide markets in most cases. Nevertheless, the larger scaled research will certainly bring more sophistication into the results. After this, further work with developing the software can be done with more confidence.

References

[1] J. Williams, “What You Need To Know About the SolarWinds Supply-Chain Attack,” Dec. 15, 2020. https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/ (accessed Jan. 17, 2022).

[2] J. D. Linton, S. Boyson, and J. Aje, “The challenge of cyber supply chain security to research and practice - An introduction,” *Technovation*, vol. 34, no. 7. Elsevier Ltd, pp. 339–341, 2014. doi: 10.1016/j.technovation.2014.05.001.

[3] M. Korolov, “Supply chain attacks show why you should be wary of third-party providers,” Dec. 27, 2021. https://www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html (accessed Jan. 16, 2022).

[4] G. E. Smith, K. J. Watson, W. H. Baker, and J. A. Pokorski, “A critical balance: Collaboration and security in the IT-enabled supply chain,” *Int J Prod Res*, vol. 45, no. 11, pp. 2595–2613, Jun. 2007, doi: 10.1080/00207540601020544.

[5] C. Colicchia, A. Creazza, C. Noè, and F. Strozzi, “Information sharing in supply chains: a review of risks and opportunities using the systematic literature network analysis (SLNA),” *Supply Chain Management*, vol. 24, no. 1. Emerald Group Holdings Ltd., pp. 5–21, Mar. 04, 2019. doi: 10.1108/SCM-01-2018-0003.

[6] M. A. Nasir, S. Sultan, S. Nefti-Meziani, and U. Manzoor, “Potential cyber-attacks against global oil supply chain,” in *2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2015*, Institute of Electrical and Electronics Engineers Inc., Jul. 2015. doi: 10.1109/CyberSA.2015.7166137.

[7] L. Urciuoli and J. Hintsa, “Adapting supply chain management strategies to security–an analysis of existing gaps and recommendations for improvement,” *International Journal of Logistics Research and Applications*, vol. 20, no. 3, pp. 276–295, May 2017, doi: 10.1080/13675567.2016.1219703.

[8] J. P. Farwell and R. Rohozinski, “Stuxnet and the future of cyber war,” *Survival (Lond)*, vol. 53, no. 1, pp. 23–40, Feb. 2011, doi: 10.1080/00396338.2011.555586.

[9] T. Radichel and S. Northcutt, “Case Study: Critical Controls that Could Have Prevented Target Breach,” Aug. 2014.

[10] B. Hawkins, “Case Study: The Home Depot Data Breach,” Oct. 2015. Accessed: Jan. 17, 2022. [Online]. Available: https://www.sans.org/white-papers/36367/

[11] S. Peisert *et al.*, “Perspectives on the SolarWinds Incident,” *IEEE Security and Privacy*, vol. 19, no. 2. Institute of Electrical and Electronics Engineers Inc., pp. 7–13, Mar. 01, 2021. doi: 10.1109/MSEC.2021.3051235.

[12] F. E. McFadden and R. D. Arnold, “Supply chain risk mitigation for IT electronics,” in *2010 IEEE International Conference on Technologies for Homeland Security, HST 2010*, 2010, pp. 49–55. doi: 10.1109/THS.2010.5655094.

[13] N. Bartol, “Cyber supply chain security practices DNA - Filling in the puzzle using a diverse set of disciplines,” *Technovation*, vol. 34, no. 7, pp. 354–361, 2014, doi: 10.1016/j.technovation.2014.01.005.

[14] NIST, “Cybersecurity Supply Chain Risk Management,” Nov. 30, 2021. https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management (accessed Jan. 16, 2022).
[15] C. Mcphee *et al.*, “Supply Chain Cyber-Resilience: Creating an Agenda for Future Research Cyber-Resilience: A Strategic Approach for Supply Chain Management Luca Urciuoli Building Cyber-Resilience into Supply Chains Cybersecurity and Cyber-Resilient Supply Chains Challenges in Maritime Cyber-Resilience Q&A. How Can I Secure My Digital Supply Chain? Technology Innovation Management Review,” 2015. [Online]. Available: www.timreview.ca
[16] S. Boyson, “Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems,” *Technovation*, vol. 34, no. 7, pp. 342–353, 2014, doi: 10.1016/j.technovation.2014.02.001.
[17] C. Colicchia, A. Creazza, and D. A. Menachof, “Managing cyber and information risks in supply chains: insights from an exploratory analysis,” *Supply Chain Management*, vol. 24, no. 2, pp. 215–240, Mar. 2019, doi: 10.1108/SCM-09-2017-0289.
[18] J. Simon and A. Omar, “Cybersecurity investments in the supply chain: Coordination and a strategic attacker,” *Eur J Oper Res*, vol. 282, no. 1, pp. 161–171, Apr. 2020, doi: 10.1016/j.ejor.2019.09.017.
[19] O. F. Keskin, K. M. Caramancion, I. Tatar, O. Raza, and U. Tatar, “Cyber third-party risk management: A comparison of non-intrusive risk scoring reports,” *Electronics (Switzerland)*, vol. 10, no. 10, May 2021, doi: 10.3390/electronics10101168.
[20] “Data Risk in the Third-Party Ecosystem Second Annual Study,” 2017.
[21] A. Ghadge, M. Weiß, N. D. Caldwell, and R. Wilding, “Managing cyber risk in supply chains: a review and research agenda,” *Supply Chain Management*, vol. 25, no. 2. Emerald Group Holdings Ltd., pp. 223–240, Feb. 24, 2020. doi: 10.1108/SCM-10-2018-0357.
[22] M. N. Faisal, D. K. Banwet, and R. Shankar, “Information risks management in supply chains: An assessment and mitigation framework,” *Journal of Enterprise Information Management*, vol. 20, no. 6, pp. 677–699, 2007, doi: 10.1108/17410390710830727.
[23] A. Davis, “Technology Innovation Management Review Building Cyber-Resilience into Supply Chains,” 2015. [Online]. Available: www.timreview.ca
[24] C. Keegan, “Cyber security in the supply chain: A perspective from the insurance industry,” *Technovation*, vol. 34, no. 7. Elsevier Ltd, pp. 380–381, 2014. doi: 10.1016/j.technovation.2014.02.002.
[25] P. N. Sindhuja and A. S. Kunnathur, “Information security in supply chains: A management control perspective,” *Information and Computer Security*, vol. 23, no. 5, pp. 476–496, Nov. 2015, doi: 10.1108/ICS-07-2014-0050.
[26] R. Putrus, “A Risk-Based Management Approach to Third-Party Data Security, Risk and Compliance,” Sep. 2017, Accessed: Jan. 17, 2022. [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-6/a-riskbased-management-approach-to-thirdparty-data-security-risk-and-compliance#:~:text=Features-,A%20Risk%2DBased%20Management%20Approach%20to%20Third%2DParty,Data%20Security%2C%20Risk%20and%20Compliance&text=As%20a%20result%2C%20the%20enterprise,of%20third%20parties%20is%20rising.
[27] A. Creazza, C. Colicchia, S. Spiezia, and F. Dallari, “Who cares? Supply chain managers’ perceptions regarding cyber supply chain risk management in the

digital transformation era," *Supply Chain Management*, vol. 27, no. 1, pp. 30–53, Jan. 2022, doi: 10.1108/SCM-02-2020-0073.
[28] T. Bandyopadhyay, V. Jacob, and S. Raghunathan, "Information security in networked supply chains: Impact of network vulnerability and supply chain integration on incentives to invest," *Information Technology and Management*, vol. 11, no. 1, pp. 7–23, Mar. 2010, doi: 10.1007/s10799-010-0066-1.
[29] S. Pandey, R. K. Singh, A. Gunasekaran, and A. Kaushik, "Cyber security risks in globalized supply chains: conceptual framework," *Journal of Global Operations and Strategic Sourcing*, vol. 13, no. 1, pp. 103–128, Feb. 2020, doi: 10.1108/JGOSS-05-2019-0042.
[30] International Organization for Standardization, "ISO27000:2018: Information technology — Security techniques — Information security management systems — Overview and vocabulary," 2018. [Online]. Available: www.iso.org
[31] International Organization for Standardization, "ISO/IEC 27001 Information technology-Security techniques," 2013.
[32] International Organization for Standardization, "ISO/IEC 27002 Information technology— Security techniques — Code of practice for information security controls," 2013.
[33] Center for Internet Security, "CIS Critical Security Controls v8," 2021. [Online]. Available: www.cisecurity.org/controls/
[34] Eurostat, "Small and medium-sized enterprises (SMEs)," *https://ec.europa.eu/eurostat/web/structural-business-statistics/information-on-data/small-and-medium-sized-enterprises*.
[35] M. Rehkopf, "User stories with examples and a template", Accessed: Apr. 15, 2023. [Online]. Available: https://www.atlassian.com/agile/project-management/user-stories

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Sander Eesmaa

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Supply chain information security management in Estonian organizations”, supervised by Kristjan Karmo.
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 – ISO27002 15.1 Information security in supplier relationships guidelines [32]

15.1 Information security in supplier relationships

Objective: To ensure protection of the organization's assets that is accessible by suppliers.

15.1.1 Information security policy for supplier relationships

Control

Information security requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented. Implementation guidance

The organization should identify and mandate information security controls to specifically address supplier access to the organization's information in a policy. These controls should address processes and procedures to be implemented by the organization, as well as those processes and procedures that the organization should require the supplier to implement, including:

a) identifying and documenting the types of suppliers, e.g., IT services, logistics utilities, financial services, IT infrastructure components, whom the organization will allow to access its information;

b) a standardised process and lifecycle for managing supplier relationships;

c) defining the types of information access that different types of suppliers will be allowed, and monitoring and controlling the access;

d) minimum information security requirements for each type of information and type of access to serve as the basis for individual supplier agreements based on the organization's business needs and requirements and its risk profile;

e) processes and procedures for monitoring adherence to established information security requirements for each type of supplier and type of access, including third party review and product validation;

f) accuracy and completeness controls to ensure the integrity of the information or information processing provided by either party;

g) types of obligations applicable to suppliers to protect the organization's information;

h) handling incidents and contingencies associated with supplier access including responsibilities of both the organization and suppliers;

i) resilience and, if necessary, recovery and contingency arrangements to ensure the availability of the information or information processing provided by either party;

j) awareness training for the organization's personnel involved in acquisitions regarding applicable policies, processes and procedures;

k) awareness training for the organization's personnel interacting with supplier personnel regarding appropriate rules of engagement and behaviour based on the type of supplier and the level of supplier access to the organization's systems and information;

l) conditions under which information security requirements and controls will be documented in an agreement signed by both parties;

m) managing the necessary transitions of information, information processing facilities and anything else that needs to be moved, and ensuring that information security is maintained throughout the transition period.

Other information

Information can be put at risk by suppliers with inadequate information security management. Controls should be identified and applied to administer supplier access to information processing facilities. For example, if there is a special need for confidentiality of the information, non-disclosure agreements can be used. Another example is data protection risks when the supplier agreement involves transfer of, or access to, information across borders. The organization needs to be aware that the legal or contractual responsibility for protecting information remains with the organization

15.1.2 Addressing security within supplier agreements

Control

All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

Implementation guidance

Supplier agreements should be established and documented to ensure that there is no misunderstanding between the organization and the supplier regarding both parties' obligations to fulfil relevant information security requirements. The following terms should be considered for inclusion in the agreements in order to satisfy the identified information security requirements:

a) description of the information to be provided or accessed and methods of providing or accessing the information;

b) classification of information according to the organization's classification scheme (see 8.2); if necessary also mapping between the organization's own classification scheme and the classification scheme of the supplier;

c) legal and regulatory requirements, including data protection, intellectual property rights and copyright, and a description of how it will be ensured that they are met;

d) obligation of each contractual party to implement an agreed set of controls including access control, performance review, monitoring, reporting and auditing;

e) rules of acceptable use of information, including unacceptable use if necessary;

f) either explicit list of supplier personnel authorized to access or receive the organization's information or procedures or conditions for authorization, and removal of the authorization, for access to or receipt of the organization's information by supplier personnel;

g) information security policies relevant to the specific contract;

h) incident management requirements and procedures (especially notification and collaboration during incident remediation);

i) training and awareness requirements for specific procedures and information security requirements, e.g. for incident response, authorization procedures;

j) relevant regulations for sub-contracting, including the controls that need to be implemented;

k) relevant agreement partners, including a contact person for information security issues;

l) screening requirements, if any, for supplier's personnel including responsibilities for conducting the screening and notification procedures if screening has not been completed or if the results give cause for doubt or concern;

m) right to audit the supplier processes and controls related to the agreement;

n) defect resolution and conflict resolution processes;

o) supplier's obligation to periodically deliver an independent report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report;

p) supplier's obligations to comply with the organization's security requirements.

Other information

The agreements can vary considerably for different organizations and among the different types of suppliers. Therefore, care should be taken to include all relevant information security risks and requirements. Supplier agreements may also involve other parties (e.g. sub-suppliers). The procedures for continuing processing in the event that the supplier becomes unable to supply its products or services need to be considered in the agreement to avoid any delay in arranging replacement products or services.

15.1.3 Information and communication technology supply chain

Control

Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain.

Implementation guidance

The following topics should be considered for inclusion in supplier agreements concerning supply chain security:

a) defining information security requirements to apply to information and communication technology product or service acquisition in addition to the general information security requirements for supplier relationships;

b) for information and communication technology services, requiring that suppliers propagate the organization's security requirements throughout the supply chain if suppliers subcontract for parts of information and communication technology service provided to the organization;

c) for information and communication technology products, requiring that suppliers propagate appropriate security practices throughout the supply chain if these products include components purchased from other suppliers;

d) implementing a monitoring process and acceptable methods for validating that delivered information and communication technology products and services are adhering to stated security requirements;

e) implementing a process for identifying product or service components that are critical for maintaining functionality and therefore require increased attention and scrutiny when built outside of the organization especially if the top tier supplier outsources aspects of product or service components to other suppliers;

f) obtaining assurance that critical components and their origin can be traced throughout the supply chain;

g) obtaining assurance that the delivered information and communication technology products are functioning as expected without any unexpected or unwanted features;

h) defining rules for sharing of information regarding the supply chain and any potential issues and compromises among the organization and suppliers;

i) implementing specific processes for managing information and communication technology component lifecycle and availability and associated security risks. This includes managing the risks of components no longer being available due to suppliers no longer being in business or suppliers no longer providing these components due to technology advancements.

Other information

The specific information and communication technology supply chain risk management practices are built on top of general information security, quality, project management and system engineering practices but do not replace them. Organizations are advised to work with suppliers to understand the information and communication technology supply chain and any matters that have an important impact on the products and services being provided. Organizations can influence information and communication technology supply chain information security practices by making clear in agreements with their suppliers the matters that should be addressed by other suppliers in the information and communication technology supply chain. Information and communication technology supply chain as addressed here includes cloud computing services.

Appendix 3 – Questionnaire

General information (organization)

1. Field of operation / business area
2. Country of operation
3. Organization size
4. Department of the respondent
5. Title/position
6. Applicable regulatory requirements & laws

Information security

1. Does the organization hold any information security certificates? Which?
2. Which ICT tools do you use to measure the organization's information security level?
3. What troubles you the most in your daily information security operations?

Supply chain information security

1. The organization has a process in place for managing suppliers

    1.1. Supplier access to information is monitored and controlled

    1.2. Inventory of suppliers is established and maintained

    1.3. It is important to keep and maintain inventory of suppliers

1.4. Supplier inventory is complex to build and maintain

1.5. Do you use any ICT tools to keep the inventory of suppliers?

1.6. Which tools?

1.7. Key benefits of the tool?

1.8. Key drawbacks of the tool?

1.9. If you could, what would you change?

1.10. What would you expect most from such a tool?

2. Supplier's information security level is assessed

2.1. It is important to evaluate suppliers' information security level

2.2. Supplier information security level is complex to evaluate

2.3. Evidence to verify the information security level is collected

2.4. Do you use any ICT tools to evaluate suppliers' information security level?

2.5. Which tools?

2.6. Key benefits of the tool?

2.7. Key drawbacks of the tool?

2.8. If you could, what would you change?

2.9. What would you expect most from such a tool?

3. Minimum information security requirements and controls are set for suppliers

3.1. It is important to set such requirements and controls

3.2. It is complex to define and set such requirements and controls

3.3. These requirements are documented in an agreement and signed by all parties

3.4. Adherence to those requirements is monitored

3.5. It is important to monitor the adherence to information security requirements

3.6. It is complex to monitor the adherence to information security requirements

3.7. Evidence is collected to verify the adherence to those requirements

3.8. Do you use any ICT tools to monitor the adherence to information security requirements?

3.9. Which tools?

3.10. Key benefits of the tool?

3.11. Key drawbacks of the tool?

3.12. If you could, what would you change?

3.13. What would you expect most from such a tool?

4. Has the organization been requested to be compliant with certain set of information security requirements or regulations by its partners?

4.1. How do you map and track these requests?

4.2. How often do you receive such requests?

4.3. How long does it usually take to put together an answer per request?

4.4. Is evidence requested to validate answers to the requests?

Appendix 4 – Unique functional requirements

The software must enable users to categorize types of suppliers.
The software must allow users to manage the whole supplier lifecycle.
The software must provide overview of supplier accesses to information and systems.
The software must allow to define and monitor compliance to minimum information security requirements for each supplier.
The software must allow to include evidence that verifies the adherence to minimum information security requirements.
The software must allow to link and manage supplier contacts and representatives that will be allowed access to organization's systems or data.
The software must allow to categorize supplier as sub-contractors and link/unlink them to existing supplier relationships.
The software must provide automation where possible.
The software must allow central supplier management – including contracts and inventory.
The software must enable proactive approach to supply chain information security management.
The software must offer overview from both business (e.g., agreements) and information security aspects (e.g., adherence to requirements).
The software must provide overview of issues and incidents associated with each supplier.
The software must enable to ingest supplier audits and corresponding mitigation plans where applicable.
The software must offer a cloud and on-prem based solutions.

The software must withstand management of extensive number of suppliers.
The software must support integration with other systems.
The software must keep an archive and provide users access to historical data.
The software must use OSINT to enrich the information about the supplier's information security maturity level.
The software must allow users to build, send, receive, and manage information security questionnaires.
The software must have the option to perform auditing operations of the information gathered from suppliers.
The software must follow information security best practices (e.g., MFA, encryption) by being compliant to applicable information security standards (e.g., ISO27001).
The software must allow assessing suppliers based on selection of information security standards (e.g., ISO27001, NIST, HIPAA, PCI DSS, CIS Controls).
The software must display quick view of the supplier's information security maturity level value.
The software must allow acceptance of information security certificates which in turn will automatically make the given supplier compliant to a set of requirements.
The software must have the option to build automated workflows that must be flexible enough to fit different organization needs.
The software must also allow to accept incoming compliance checks and keep the lifecycle of those business flows too.
The software must allow generating quick report on suppliers.
In addition to supplier information security management, the software must also be able to store and manage the organization's information security level.

Appendix 5 – User stories

User Story 1.1:

As a supply chain manager, I want to categorize suppliers by their types, so that I can better organize and manage them according to their roles and importance in the supply chain.

User Story 2.1:

As a supply chain manager, I want to manage suppliers through their entire lifecycle, from onboarding to termination, so that I can maintain a consistent and effective supply chain.

User Story 3.1:

As a supply chain manager, I want to view an overview of supplier accesses to information and systems, so that I can ensure appropriate access controls are in place and monitor any unauthorized access.

User Story 4.1:

As a supply chain manager, I want to define and monitor compliance to minimum information security requirements for each supplier, so that I can ensure they meet our organization's security standards.

User Story 5.1:

As a supply chain manager, I want to upload and attach evidence that verifies a supplier's adherence to minimum information security requirements, so that I can maintain a record of compliance.

User Story 6.1:

As a supply chain manager, I want to link and manage supplier contacts and representatives who are allowed access to our organization's systems or data, so that I can ensure proper access controls are in place and there are no unauthorized accesses.

User Story 7.1:
As a supply chain manager, I want to categorize suppliers as sub-contractors and link or unlink them to existing supplier relationships, so that I can manage the complexity of our supply chain and maintain visibility of all parties involved.

User Story 8.1:
As a supply chain manager, I want the software to automate tasks where possible, so that I can save time and reduce manual effort in managing information security in the supply chain.

User Story 9.1:
As a supply chain manager, I want a centralized system to manage suppliers, including contracts and inventory, so that I can efficiently track and maintain information in one place.

User Story 10.1:
As a supply chain manager, I want the software to enable a proactive approach to supply chain information security management, so that I can identify and address risks before they become critical issues.

User Story 11.1:
As a supply chain manager, I want an overview of both business and information security aspects for each supplier, so that I can make informed decisions and manage risks effectively.

User Story 12.1:
As a supply chain manager, I want to view an overview of issues and incidents associated with each supplier, so that I can analyse and address any risks or vulnerabilities in our supply chain.

User Story 13.1:

As a supply chain manager, I want to ingest supplier audits and corresponding mitigation plans to the system where applicable, so that I can track and manage compliance efforts effectively.

User Story 14.1:
As a supply chain manager, I want the software to offer both cloud and on-prem based solutions, so that I can choose the deployment model that best fits my organization's needs.

User Story 15.1:
As a supply chain manager, I want the software to withstand management of an extensive number of suppliers, so that I can scale my supply chain management efforts as needed.

User Story 16.1:
As a supply chain manager, I want the software to support integration with other systems, so that I can seamlessly connect it with existing tools and processes in my organization.

User Story 17.1:
As a supply chain manager, I want the software to keep an archive and provide users access to historical data, so that I can track and analyse changes over time.

User Story 18.1:
As a supply chain manager, I want the software to use OSINT to enrich the information about the supplier’s information security maturity level, so that I can make better informed decisions.

User Story 19.1:
As a supply chain manager, I want the software to allow me to build, send, receive, and manage information security questionnaires, so that I can effectively assess the security posture of my suppliers.

User Story 20.1:

As a supply chain manager, I want the software to have the option to perform auditing operations on the information gathered from suppliers, so that I can validate the accuracy and reliability of the data.

User Story 21.1:
As a supply chain manager, I want the software to follow information security best practices and be compliant with applicable information security standards, so that I can trust its security and integrity.

User Story 22.1:
As a supply chain manager, I want the software to allow me to assess suppliers based on a selection of information security standards, so that I can evaluate their compliance with various frameworks relevant to my organization.

User Story 23.1:
As a supply chain manager, I want to see a quick view of the supplier's information security maturity level value, so that I can easily assess their overall security posture.

User Story 24.1:
As a supply chain manager, I want the software to allow the acceptance of information security certificates, which will automatically make the given supplier compliant to a set of requirements, simplifying the compliance process.

User Story 25.1:
As a supply chain manager, I want the software to offer the option to build automated workflows that are flexible enough to fit different organizational needs, so that I can streamline supply chain management processes.

User Story 26.1:
As a supply chain manager, I want the software to accept incoming compliance checks and manage the lifecycle of those business flows, so that I can efficiently handle incoming information and maintain up-to-date records.

User Story 27.1:

As a supply chain manager, I want the software to generate quick reports on suppliers, so that I can easily share insights and make informed decisions.

User Story 28.1:
As a supply chain manager, I want the software to store and manage my organization's information security level in addition to supplier information security management, so that I can maintain a comprehensive view of our overall security posture.