



Cyber Security for Europe

D9.25

Supply Chain Security Recommendations 2

Document Identification	
Due date	31 October 2022
Submission date	24 January 2023
Revision	1.0

Related WP	WP9	Dissemination Level	PU
Lead Participant	TDL	Lead Author	David Goodman (TDL)
Contributing Beneficiaries	NTNU, TDL, ATOS, UM, JAMK	Related Deliverables	D9.12

Abstract: This report is the first deliverable in the sequence of two deliverables that make security recommendations to the supply chain. The recommendations are made specifically focusing on small and medium-sized enterprises so to protect against cyber challenges that could arise due to the integration of emerging technologies into the supply chain.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929. This document and its content are the property of the CyberSec4Europe Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the CyberSec4Europe Consortium and are not to be disclosed externally without prior written consent from the CyberSec4Europe Partners. Each CyberSec4Europe Partner may use this document in conformity with the CyberSec4Europe Consortium Grant Agreement provisions and the Consortium Agreement.



The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Executive Summary

This report continues the narrative, initiated in the first report in this two-part series, to pull together the work on supply chain and related activities from across the project, notably roadmapping trends and challenges, both technological and business-related from WP4, the work on blockchain-based supply chain demonstrator use cases in WP5, the cybersecurity awareness review and recommendations from WP9 as well as a thorough analysis of thirteen EU regulations and directives from the dual perspectives of supply chain and SMEs.

The methodology adopted was to set the scene by identifying the existing supply chain threats and their impact as well as the challenges to supply chain cybersecurity - and the opportunities arising. We reviewed the recommendations from the previous report, concluding that in the most part their ambition continued to be valid. going forward. The rest of the report focussed on providing a new set of recommendations from the perspectives of technology, training and awareness, as well as the perceived gaps in the regulatory sphere.

Document information

Contributors

Name	Partner
Michael Herburger	FHO
Carina Hochstrasser	FHO
Jani Päijänen	JAMK
Sunil Chaudhary	NTNU
Vasileios Gkioulos	NTNU
Martin Wimmer	SIE
Ricarda Weber	SIE
David Goodman	TDL
Marko Kompara	UM
Rodrigo Roman	UMA
Cristina Alcaraz	UMA

Reviewers

Name	Partner
Jozek Vyskoc	VAF
Jarno Salonen	VTT

History

Version	Date	Authors	Comment
0.1	26 October 2022	David Goodman	First draft
0.2	17 November 2022	All	Second draft
0.3	8 December 2022	David Goodman	Third draft
1.0	24 January 2023	Ahad Niknia	Final check, preparation, and submission

Table of Contents

1	Introduction.....	1
1.1	Objective, scope and methodology	2
1.2	Target audience.....	3
2	Setting The Scene	3
2.1	Threats and risks.....	3
2.1.1	Existing supply chain threats	3
2.1.2	Impact of threats on supply chains.....	5
2.1.3	Challenges to supply chain cybersecurity	6
2.2	Opportunities.....	7
3	Recommendations	12
3.1	Introduction.....	12
3.2	Review of previous recommendations.....	13
3.2.1	General IT security recommendations	13
3.2.2	Legal recommendations	13
3.2.3	Standards recommendations.....	14
3.2.4	Security recommendations derived from CyberSec4Europe work	15
3.2.5	Tools recommendations	16
3.2.6	Recommendations to the EU.....	17
3.2	Technology.....	17
3.2.1	What opportunities are seen for supply chain security	17
3.2.2	Evaluation / Results gained from project	19
3.3	Organisational / training recommendations.....	25
3.3.1	Guidelines and best practices	25
3.3.2	Awareness and Training.....	28
3.4	Regulation Analysis	29
3.4.1	Introduction	29
3.4.2	Analysis per regulation	31
3.4.3	Recommendation/gaps	54
4	Summary and next steps	57
4.1	A summary of threats / risks, opportunities and recommendations	57
4.2	Recommended next steps for EU funding and/or regulation.....	57
4.2.1	Regulatory	57
4.2.2	EU funding	57
4.2.3	Training and education.....	58
5	References	59

List of figures

Figure 1: flow of goods and funds.....	20
Figure 2: SCH-UC2 software architecture	22
Figure 3: Workflow to validation	25

List of Acronyms

<i>A</i>	AEO	Authorised Economic Operator
	AI	Artificial Intelligence
<i>B</i>	BSI	British Standards Institution
	BYOD	Bring Your Own Device
<i>C</i>	CA	Certification Authority
	CCS	Centre for Cyber Security
	CISA	Cybersecurity and Infrastructure Security Agency
	CPS	Cyber-Physical System
	CRM	Customer Relationship Management
	C-SCRM	Cybersecurity Supply Chain Risk Management
<i>D</i>	DLT	Distributed Ledger Technology
<i>E</i>	ENISA	European Union Agency for Cybersecurity
	EU	European Union
<i>G</i>	GDPR	General Data Protection Regulation
<i>H</i>	HLF	Hyperledger Fabric
<i>I</i>	ICT	Information and Communication Technology
	IEC	International Electrotechnical Commission
	IoT	Internet of Things
	IP	Intellectual Property
	ISO	International Organisation for Standardisation
	IT	Information Technology
<i>M</i>	ML	Machine Learning
	MSP	Membership Service Provider
<i>N</i>	NCSC	National Cyber Security Centre
	NICCS	National Initiative for Cybersecurity Career and Studies
	NIS	Network and Information Security

	NIS1	NIS 2016
	NIS2	Revised NIS
	NIST	National Institute of Standards and Technology
<i>O</i>	OES	Operators of Essential Service
	OT	Operational Technology
	OTTF	Open Trusted Technology Forum
<i>P</i>	PDC	Private Data Collections
	PII	Personally Identifiable Information
	PKI	Public Key Infrastructure
<i>S</i>	SBS	Small Business Standards
	SITA	Société Internationale de Télécommunications Aéronautiques
	SME	Small and Medium Sized Enterprise

Glossary of Terms

R **Risk**

A combination of cyber threat probability and the potential loss or harm related to technical infrastructure or the use of technology within an organisation.

T **Threat**

A cybersecurity circumstance or incident or act with the potential to cause harm by a way of its outcome.

V **Vulnerability**

Weaknesses in a cyber system that can be exploited by hackers or malicious programmes.

1 Introduction

In the first of these two reports on supply chain security recommendations, we presented the context of supply chains generally, as being physical, digital or, as is increasingly prevalent, a combination of both. Specifically, we identified the threat posed to digital supply chains from cyber attacks, noting a 78% year-on-year increase in 2018. However, according to a recent report from French reinsurer SCOR, the volume of attacks grew by 430% in 2021. A similar escalation is observed according to ENISA:

It is estimated that there will be four times more supply chain attacks in 2021 than in 2020. With half of the attacks being attributed to Advanced Persistence Threat (APT) actors, their complexity and resources greatly exceed the more common non-targeted attacks, and, therefore, there is an increasing need for new protective methods that incorporate suppliers in order to guarantee that organizations remain secure.

We stated that the main objective of the report was to make cybersecurity recommendations for supply chains specifically focusing on small and medium-sized enterprises (SMEs) which represent 99% of the enterprises in the European Union and play important roles in supply chains. Not only are SMEs perceived as being the most vulnerable links in supply chains, but SMEs also inevitably have to play catch-up with large organisations undergoing digital transformations and implementing new state of the art or emerging technologies, particularly those based on artificial intelligence (AI) / machine learning (ML) techniques.

We went on to identify and analyse some of the types of threats facing supply chains:

- **Cyber-physical attack**, defined as “a security breach in cyberspace that adversely affects physical space.”
- **Data breach and GDPR non-compliance**, where data breach is any exposure to enterprise confidential, sensitive or protected data to unauthorised entities. It can occur due to technology vulnerabilities or human behaviours, although in most cases human behaviours are found to be responsible.
- **Supply chain impersonation attack**, defined as, “an attack in which an adversary successfully assumes the identity of one of the legitimate parties in a system or in a communications protocol.”
- **Business (or corporate) identity theft**, a type of fraud that involves criminals stealing a company’s identity and using it to commit fraud.

In addition, we referenced the threats and risks originating from the implementation of, for example, AI, big data, Internet of Things (IoT).

We followed this by a breakdown of the impacts of cyber attacks on the supply chain, which were derived from the CyberSec4Europe roadmapping work on supply chains and categorised as harm impacting on operations, assets, individuals, other organisations and nations. All of these, *in extremis*, could be seen to have fairly devastating, long term physical, financial, operational or reputational impacts on multiple organisations - as is often the case with cyber attacks.

The challenges to supply chains, in the first instance, are highly dependent on the participating organisations, according to their size, type, location, resources and cybersecurity awareness and

preparedness. Beyond that, we observed that organisations are under constant pressure, due to relentless business competition, to innovate and evolve so that they can offer their products and services at a lower cost while maintaining high quality and on time delivery. Consequently, businesses are continuously transforming their supply chains to meet modern customer demands utilising emerging technologies, such as cyber-physical systems (CPS), AI and machine learning (ML), IoT, big data, cloud computing, and augmented and virtual reality are being integrated into digital supply chains. Along with common threats like malware attacks, data breaches, information distortion, un(intentional) vulnerabilities, and malicious updates/maintenance, forward-looking organisations also inherit new threats particular to these emerging technologies.

The next section explored two supply chain security scenarios based on work carried out elsewhere in CyberSec4Europe related to supply chain, primarily roadmapping from WP4 and the supply chain demonstrator use cases in WP5.

The scenarios described highlight how the use of permissioned blockchain technology and workflow enforcement utilising smart contracts support securing supply chains across organisations without the need for a trusted third party

In addition to a description, each scenario also contained:

- Potential weaknesses and their exploitation
- The impact on SMEs
- Lessons learned
- Roadmap solutions

The final section of the first report proposed a series of recommendations broken down into the following categories, all in the context of supply chain cybersecurity:

- General IT security
- Legal
- Standards
- Security derived from CyberSec4Europe
- Tools

The final set of nine recommendations, derived from the roadmapping work on supply chains but also in the context of the demonstrator use cases, was directed to the EU.

1.1 Objective, scope and methodology

The objective of this report is, besides building on what was presented in the first report, is to present a cohesive narrative that embraces the scope and content of all the work carried out in CyberSec4Europe across different work activities that include:

- **WP3** has evolved a series of software assets with the intention of supporting the application demonstrators, including supply chain
- **Task 4.5** covers many different aspects and dimensions pertaining to the research challenges associated with supply chains

- **Task 5.2** includes the two supply chain use case demonstrators referenced in the first report. Their inclusion here is benefitted by the conclusion of the work with the accompanying lessons learned and recommendations
- **Task 7.2** sits in a work package focussed on tools, but of particular interest for supply chains is the role that cyber ranges and in particular the Flagship exercises can play in supporting training
- **Task 9.4** is a substantial activity tasked with raising awareness in general but with particular reference to the challenges associated with improving SME awareness, featuring the availability of suitable programs and finding the right channels for large scale communication. The crucial role of SMEs in supply chains and their perceived unintentional vulnerabilities is the rationale for this series of reports
- **Task 9.6** gathers recommendations from across the project in the context of policy that can be promulgated to the appropriate policy makers and regulatory bodies at either a national, European or international level. This report has the opportunity of providing input into the final set of policy briefs.

1.2 Target audience

The main objective of this report is to make cybersecurity recommendations to the supply chain specifically focusing on SMEs that represent 99% of the enterprises in the EU and play important roles in supply chains.

Hence, the audiences we are addressing with this report range

- from policy makers and strategists associated with the EU and its various agencies from the European Commission to the European Cybersecurity Competence Centre;
- to small to mid-size SMEs, with a focus on the lower end of that category as mid-size may already encompass those companies having sufficient resources and economic strength to address a broad range of cybersecurity issues.

2 Setting The Scene

2.1 Threats and risks

2.1.1 Existing supply chain threats

As we have mentioned, organisations in a supply chain are heavily dependent on the Internet and information and communication technology (ICT) infrastructures. This situation opens the avenue to multiple cyber attacks that not only target such infrastructures, but also will make use of such infrastructures to increase their extent and impact. In the previous report in this series, we described various such threats, including *cyber-physical attacks*, *GDPR non-compliance and data breaches*, *supply chain impersonation attacks* and *business identity theft*.

- The notion of *cyber-physical attacks*, or “a security breach in cyberspace that adversely affects physical space” is unfortunately a very real threat. We can consider that the Stuxnet worm, discovered in 2010, was the first known malware that actively damaged physical infrastructures. The potential impact of this category of threats caused by nation-state actors is increasing over time [Lemay18], and it is in fact used to complement physical warfare – as seen in the Russo-Ukrainian war [Nozomi22]. However, nation-state actors are not the only entities that can cause havoc in a physical space. For example, leaked logs from the Conti ransomware-as-a-service

group explicitly described IoT devices as an essential initial attack surface [Forescout22]. Even if these attacks targeted mostly ICT infrastructures, there is no assurance that physical infrastructures will not be attacked in the near future by any kind of actor, using any means necessary (from IoT entities to other connected objects such as autonomous vehicles).

- Regarding *GDPR non-compliance*, companies working on supply chain ecosystems must consider that their operations require collecting and managing data – which will need protection in compliance with the GDPR. Although adoption was slow at the beginning [GDPR19], compliance seems to be gradually increasing in countries with a high multinational company presence such as Ireland [McCann22]. Additionally, the GDPR has brought multiple benefits beyond its initial goal, such as improving the behaviour of companies in regard to data management and directly influencing the laws of other nations. Still, there are various challenges that need to be tackled for the future, including better enforcement of the GDPR [EDPS22] and the availability of well-trained professionals and tools that facilitate their tasks [Matt22].
- As for *data breaches*, or the exposure of enterprise confidential, sensitive or protected data to unauthorised entities, they are becoming more and more important. Traditionally, the involvement of a multitude of diverse actors increases the possibility of multiple cybersecurity threats: on average, an enterprise shares its sensitive data with approximately 583 third parties [Alickaj18]. However, the reliance on ICT infrastructures and software is bringing new challenges, as criminals can target key services to extract as much information as possible from a critical infrastructure sector. For example, SITA – an air transport industry IT provider that serves 90% of airlines – suffered a breach that compromised the personal data of millions of airline customers [SITA21]. Moreover, an attack to one actor or supplier can escalate to attacks against the core business network on an entity. One example of this is the cyber attack that targeted the SolarWinds company, whose Orion monitoring and management tool was manipulated in order to include a malicious backdoor. As a result, the Orion tool was used by malicious entities to spy on companies and organisations [Peisert21].
- Finally, we need to consider the impact of impersonation, or “an attack in which an adversary successfully assumes the identity of one of the legitimate parties (in a system or in a communications protocol)” [Adams05]. There are two main variations of this: *supply chain impersonation attacks* (impersonation on digital space) and *business identity theft* (impersonation on physical space). Attacks related to impersonation are on the rise, as social engineering attacks – exploitation of human error to gain unauthorised access – remain one of the most important attack vectors as of 2022 [ENISA22b]. One clear example of this is business e-mail compromise (BEC), where the attacker impersonates business owners and executives for financial gain. Other examples include phishing (non-targeted malware campaigns) from trusted accounts (e.g., hijacked colleagues), more creative solutions to steal users’ credentials such as the use of a malicious QR code, or even the use of AI-based automation [ENISA22b].

Beyond the threats described in the previous report in this series, and updated above, there are other threats whose importance require further study. Recent events highlight the importance of considering the dual nature of existing supply chains, where the goods that are managed and processed can also be digital, and where data and algorithms are the equivalent of raw materials and production processes. In addition, we also must consider how attackers compromise ICT infrastructures with the goal of sabotaging critical elements of the supply infrastructure. Therefore, it is essential to take into consideration the existence of threats such as *software supply chain attacks* and *sabotaging attacks*.

- *Software supply chain attacks* are on the rise. Various industrial reports describe how there has been an average annual increase of 742% in software supply chain attacks over the 2019-2022 period [Sonatype22]. Even more, according to ENISA, in 2021 66% of reported incidents against supply chain ecosystems focused on the suppliers' code [ENISA21]. Many of these attacks were caused by attacks against open-source libraries, such as Log4J (an open-source Java library for logging error messages in applications), while other attacks focused on targeting specific software infrastructures – such as the Orion tool mentioned above, or the Codecoy breach (a company that provided software testing tools and that was breached by malicious actors). The severity of this problem has even spilled over into the political arena. The US administration included in the '2021 Executive Order on Improving the Nation's Cybersecurity' the need for sharing software bill of materials (SBOM) information when software is being delivered across organisational boundaries [USBill21]. Also, China's reporting regulations now require the reporting of vulnerabilities into a government authority for review prior to the vulnerability being shared – which according to Microsoft has caused a surge in zero-day based attacks [MS22].
- The main purpose of *sabotaging attacks* is to disable part of the supply chain infrastructure (usually through ransomware-like attacks), greatly impacting the availability of processed goods available to customers and providers. In fact, not only have there been several high-profile cases over the last few years, but also, according to ENISA ransomware has adapted and evolved, becoming more efficient and more devastating [ENISA22a]. One clear example of such high-profile attacks was the Colonial Pipeline Breach, where – after stealing the information from the company – the attackers started a ransomware attack. This attack forced the company to shut down its fuel pipeline, which in turn affected the fuel supply to the East Coast of the USA. Other examples include the Kaseya cyber attack, where a software supply chain attack was used to manipulate a remote management tool to distribute ransomware that affected over a thousand businesses, and the JBS USA cyber attack, where the ICT infrastructure of a global meat processing company had to be shut down for several days – which caused a shortage in the US meat supply and driving wholesale meat prices up by as much as 25 per cent.

2.1.2 Impact of threats on supply chains

All the previously mentioned threats can have a powerful impact on our supply chains, leading to operational, financial, and reputational damages that may not be completely recoverable or repairable. An overview of the potential impacts to our society resulting from a supply chain failure is presented here, extracted from CyberSec4Europe deliverable D4.5 (pp. 81-82 [CS4ED45]).

Impacts on society due to a supply chain failure

- *Harm to operations:*
 - *Inability to perform current missions/business functions:* attacks through the supply chain become commonplace, and organisations are always vulnerable.
 - *Inability, or limited ability, to perform missions/business functions in the future:* as organisations are always vulnerable, it becomes impossible to fully recover from continuous attacks.
 - *Harms (e.g. financial costs, sanctions) due to noncompliance:* complex regulations cannot be implemented.

- *Relational harms*: trust relationships between organisations are lost, because managing supply chain threats has become an impossible task.
- *Harm to assets*:
 - *Damage to or loss of physical facilities*: terrorist attacks take advantage of supply chain vulnerabilities to damage physical facilities, also causing human casualties.
 - *Damage to or loss of information systems or networks*: traditional cyber attacks, such as ransomware, relentlessly disable the underlying ICT infrastructure that supports the supply chain ecosystem.
 - *Damage to or loss of component parts or supplies*: it becomes impossible to manage threats against physical/digital assets when the supply chain is transformed into a chaotic supply web.
 - *Damage to or loss of information assets*: various information assets are tampered with by malicious adversaries rendering the know-how and intellectual property of companies useless.
 - *Loss of intellectual property*: IP routinely gets stolen from corporations and governments.
- *Harm to individuals*:
 - *Injury or loss of life*: counterfeited or altered products affect people either directly or indirectly.
 - *Physical or psychological mistreatment*: the public cannot trust the safety of the products they use in their daily lives.
- *Harm to other organisations*:
 - *Relational harms*: The interconnected nature of supply chains causes damage to all actors involved in this vertical if the ecosystem can no longer be trusted.
- *Harm to the nation*
 - *Relational harms*: loss of trust relationships with other nations, loss of national reputation, loss of national security due to the impact on the critical infrastructure.

In fact, without strengthening the security of EU supply chain actors and processes against the previously mentioned threats on all fronts (from technology to standardisation), it will not be possible to tackle the challenges related to the secure digitalisation of supply chains, which are crucial for the digital sovereignty of Europe – and an explicit goal of the EU's 'Cybersecurity Strategy for the Digital Decade' [EUCS20]. Such challenges include the secure supply of clean and affordable energy and (raw) materials, ensuring balanced responsibilities for all market players depending on their position in the supply chain, and certifying that all items that are supplied are indeed exempt from security concerns.

2.1.3 Challenges to supply chain cybersecurity

There are several factors that pose challenges to achieving sufficiently secure supply chain infrastructures. Some of these factors were discussed in the previous report in this series, such as the *heterogeneity in the participating organisations*, and the *integration of emerging technologies*.

- *Organisation heterogeneity*. There are several issues related not only to the size of the organisations but also with the relationship between all of them. For example, SMEs and micro-

SMEs might not have all the necessary resources to integrate the cybersecurity mechanisms that can provide protection against the previously defined threats. In addition, due to the complex web of interactions between multiple tiers of public and private stakeholders, it is very challenging to ensure not only the cybersecurity level of these third parties, but also to protect the cybersecurity of the organisation if one of such parties is affected by a cyber attack. Finally, it is also important to consider the need to train a skilled workforce and develop the necessary tools that are prepared to react against extremely dynamic adversaries.

- *Integration of emerging technologies.* Businesses are integrating various emerging technologies due to the digitalisation of supply chains and the need to integrate novel services to improve service quality while maintaining or lowering operational costs. Examples of such emerging technologies are cloud and Edge computing, Internet of Things (IoT), artificial intelligence (AI), big data, augmented and virtual reality, and digital twins. However, the integration of these technologies brings specific security and privacy challenges related to the inherent features of every technology [CS4ED45]. These challenges are mostly related to
 - the existing security and privacy challenges of the underlying technologies e.g., shared ecosystems in cloud/Edge computing, malfunctioning or weak components in IoT;
 - the integration of IT and OT technologies which bring novel attack vectors to a previously isolated environment, even more critical in the case of digital twins due to their direct interconnection with the virtual and physical environments;
 - the protection of vast amounts of sensitive information and models e.g., secure and private data management, source validation and filtering in big data and AI; and
 - other novel issues related to the close interaction between physical and digital environments e.g., digital reality not matching the physical world in augmented reality situations.

However, there are other novel aspects that must be discussed related to the previously mentioned threats and the different dimensions of the security of supply chains, aspects that were initially analysed in CyberSec4Europe deliverable D4.5 (cf. Section 4.6 [CS4ED45]) and that are summarised here.

- *Digitalisation and COVID-19.* The rise of COVID-19 increased the digitalisation and the evolution of supply chain policies, including the regionalisation of trade and production networks, the focus on proximity to consumers, the implementation of better data visibility controls and the increased use of automation technologies in manufacturing [McKinsey20]. However, this sudden digitalisation has directly impacted the security of supply chains, due to the increased risk caused by introducing poorly protected partners into their supply chains, integrating novel technological solutions that increase the attack surface and implementing remote work policies in environments where it was not common beforehand.
- *Climate change.* It is essential to reduce the impact of supply chains in the environment. There are various technologies that can be used to optimise supply chains and eliminate waste, such as energy-conscious blockchain technologies for traceability and data visibility and digital twins for predictive maintenance. However, as with the COVID-19 digitalisation push, this integration of the digital technologies increases the attack surface of digital supply chains, and as such increase the need to incorporate defensive and proactive mechanisms against existing threats.

2.2 Opportunities

We are increasingly witnessing how the supply chain is being subjected to more globalised and interconnected management, implying a digital transformation that leads to multiple types of attacks and incidents [ENISA21, SCOR2022]. Many of the threats are designed to have a large-scale effect, the impact of which is mainly due to the heavy reliance on new technologies, the application of the Internet (as a means of connection) and the recent acceptance of cryptocurrencies as a way of making market. In turn, the effect of the COVID-19 pandemic and the unpleasant situation in Ukraine have not contributed (and do not contribute) to reducing the number of threats and their effects [Alicke2020, SCOR22]. For example, the pandemic has created a new teleworking model that has motivated attackers to exploit the different types of vulnerabilities by taking advantage of the different attack surfaces. The hostile nature of many of the computer systems installed in homes for teleworking and the way in how they are connected to the supply chain has triggered the rate of successful cyber attacks; many more than if they had been launched from the corporate network. The security measures are completely different.

Indeed, several lessons learned in the post-pandemic period have emerged:

- (i) teleworking opens up a new way of doing business and new opportunities for SMEs, but also
- (ii) new opportunities for attackers to exploit security breaches with impact on the value and supply chain.

According to [SCOR22], cyber attacks in supply chains grew by no less than 430% in 2021, where the majority of incidents (66%) were related to the exploitation of supplier software bugs and zero-day vulnerabilities to subsequently compromise targeted customers. Numerous real examples have demonstrated this, especially since 2020 with NetBeans, Sopra Steria, Accellion, SolarWinds, Mimecast, Xcode, Windows HCP, Codevov, Kaseya, log4Shell, Thalès and Okta, among many others; most of them reaching many other companies and others reaching end targets. In addition, the current ransomware trend presents an average ransom demand of \$5 million per case, increasing the complexities in dealing with or mitigating the effects of an attack [PaloAlto22].

Moreover, the “digital supply chain” effect can have a greater effect on those critical control systems mounted on top of business systems whose services are considered essential for society, such as water, power or gas. As indicated in [SCOR22], the IT-OT effect without security requirements and without following the good practices could allow attackers to first attack the IT network and then penetrate the OT network to take control of the most critical resources of the system or of the sector. Uncontrollable or untested security patches, outsourcing of services under any trust criteria with respect to third parties, and remote maintenance lead to multiple kinds of problems discussed in previous sections.

It is therefore easy to understand the relevance of deploying standards and regulatory frameworks to impose good practices, in which it is necessary to involve the various communities to define more robust and viable protection and transparency measures. However, this need is neither new nor recent. The report described in [SCOR22] shows a list of contributions provided by industries, organisations and regulatory bodies, which cooperate from a global and coordinated perspective. For example, the BoostAeroSpace was founded in 2011 by Airbus, Dassault Aviation, Safran and Thales, to collaborate and develop a set of European aerospace and defence industry supply chain security standards and increase the cyber protection levels of aerospace suppliers. Regulatory measures are also being put in place, such as the GDPR on supply chain (addressing risks posed by third parties, human rights and transparency in the supply chain [GDPR21a]), the NIS2 Directive (addressing cybersecurity implications in the supply chain [NIS22022]), or the UN Cybersecurity Rules, Standards and Principles for Responsible State Behavior (defining the set of security requirements to protect the digital supply chain); but also standardisation frameworks, best practices and recommendations. For example, we can find the

cybersecurity framework which extracts the set of requirements needed to address and mitigate supply chain risks [NIST2018] defined by the National Institute of Standards and Technology (NIST) and its good practices for risk management detailed in [NIST2022a], as well as ENISA with its recommendations on risks and threats in the sector [ENIS2021].

To understand the EU's level of preparedness in solving the problems of digital transformation and interconnectivity of supply chain entities and to identify major opportunities and challenges in this space, the following table lists some benefits and drawbacks involved in adapting the new European proposals and initiatives, as well as the opportunistic advantages they could bring to the global market. The analysis, extracted from CyberSec4Europe deliverable D4.5 (pp. 95-98 [CS4ED45]), is based on the traditional SWOT (strengths, weaknesses, opportunities, and threats) methodology:

Strengths	<ul style="list-style-type: none"> • <i>Regulated business strategies and transparency:</i> digital transformation places European producers and consumers in an agile economy, enabling European industries and SMEs to compete in a highly globalised market. However, this capability in turn enables the EU to have the additional power to change the way of producing and distributing services, assets or goods to comply with standards and regulations in a transparent way. • <i>Knowledge and preparation for the new business model and market:</i> the EU has strong and solid educational standards, and European SMEs and academia are ready to demonstrate their design and engineering capabilities to address new market needs and risks. • <i>Increased interest in research and funding:</i> there are a significant number of instruments to fund and support research and scientific progress in the field of supply chain and end-user protection. This level of funding is even more appreciable in the field of (cyber)security, where a significant number of European projects have recently been funded, such as CyberSec4Europe. • <i>Globalisation and industrial leadership:</i> there are already companies that are major references worldwide that can enforce protection requirements at European level, and in their respective fields of application, in their value and supply chain, as is the case with industrial machinery and automotive. • <i>Support for standardisation and certification:</i> European organisations and companies are part of the Open Trusted Technology Forum (OTTF) seeking to find ways to develop open standards and certification programs that address integrity and security issues in the supply chain. • <i>Other supports from European organisations:</i> international organisations, such as ENISA, offer a set of security recommendations and fundamental guidelines to consider in each sector and application domain, such as supply chain integrity [ENISA 2015], healthcare and Industry 4.0
------------------	--

	<p>[ENISA2019a], and for secure ICT procurement of electronic communications [ENISA 2014].</p>
<p>Weaknesses</p>	<ul style="list-style-type: none"> • <i>Lack of leadership in some strategical sectors:</i> some IT sectors, such as software and consumer electronics, show a certain lack of leadership at the European level [Schäfer2018]. There is a special need to <ul style="list-style-type: none"> (i) define security and privacy standards when privacy issues are also needed to control and trace assets and goods from a reasonable perspective, as well as to (ii) provide techniques for testing, certification and future research approaches in this field. • <i>Lack of supply chain security standards:</i> although there are already attempts and much progress in terms of regulations and recommendations (as seen above), there is still no catalogue of measures at the EU level that uniformly regulates supply chain security in Europe (and its relationship with other countries). This lack makes supply chain security compliance currently difficult to enforce in a hyper-connected society. • <i>Dependent and globalised supply chain:</i> generally, all countries depend on other countries to properly function, creating a more globalised and connected supply chain. For example, for certain European sectors, companies still need to import goods from other countries to function. Depending on certain circumstances, this dependence may lead to major risks or problems, as in the case of the war in Ukraine and the implications with Russia for exports. Problems in the distribution of essential services, such as energy and gas, have led to unforeseen changes in companies and governments [Ashraf2022].
<p>Opportunities</p>	<ul style="list-style-type: none"> • <i>New opportunities to create economy in a greener planet:</i> related to the previous point, any unforeseen change (e.g., war in Ukraine or COVID-19), triggers changes to adapt other ways of managing the value chain, favouring another type of access to the service or product and creating innovation to support the environment; for example, the creation of local suppliers boosts the market and reduces emissions due to transportation. In addition, there is a need to know and reduce the carbon footprint of the goods involved, thus fulfilling the purposes of creating a greener planet in accordance with the existing programs and regulations, such as the European Green Deal [EUGD2019] and UN Sustainable Development Goal-7 [SGD-7] together with its Agenda 2030.

	<ul style="list-style-type: none"> • <i>New chances to generate and support digital European sovereignty and traceability:</i> the proposal to create a European "digital supply chain" can help SMEs participate in a much smarter, interactive, productive and efficient ecosystem while maintaining security and privacy requirements, and place the EU itself at the forefront of this initiative from a global perspective. In addition, digitisation and traceability of assets and goods can help predict changes in the production and distribution of goods, assets and services, and reduce any impact on society. • <i>Leverage the technical strengths of Europe and its companies to create a stronger validation and security program:</i> through experience and knowledge, it is possible to define a unified and solid validation plan that addresses the integrity of products and services (whether imported or exported) with the objective of not impacting the end customer. In addition, many of the existing cybersecurity and testing tools (SIEMs, IDSs/IPSs, blockchain networks, etc.) provided by European SMEs can help contribute today to this security and validation process. Therefore, it is essential to know the existing security tools to identify which are the most appropriate and effective ones according to the type of asset, and their main contributions and benefits from the point of view of security and privacy within the supply chain itself. • <i>Possibility to implement regulatory actions and security standards under a global approach, and more possibility to create solid and resilient society:</i> the EU can force actions, initiatives, and standards across Europe, benefiting the security and transparency of the supply chain, boosting the confidence of end customers, and promoting the reputation and prestige of suppliers. In this way, the trust placed in the quality of a product or service favours productivity, sales and the purchase of goods, contributing to a stronger and more competitive supply chain in a market globalised by Industry 4.0/5.0. In addition, this way of establishing initiatives and deploying them globally allows different countries (whether or not they are EU Members States) to manage in a coordinated and joint manner cyber attacks that could destabilise the country or countries, whether economically or politically.
Threats	<ul style="list-style-type: none"> • <i>Difficulty in adopting new regulations, standards and actions:</i> existing business models in SMEs and industries and subject to bureaucratic requirements can make it difficult to adapt to new European proposals and initiatives. Providers may, for example, want to use only their own validation mechanisms and processes, and not adhere to a common

standard, or simply not want to contribute to the concept of European digital sovereignty. This would, in turn, complicate the traceability proposal and the launch of new validation and standardisation initiatives. Moreover, governmental institutions could support this refusal, as each country usually establishes its own policies and standards, which would further complicate the EU proposal.

- *Economic and scientific impact:* dramatic situations such as the war in Ukraine or the pandemic may divert the EU's current interest to fund other more urgent purposes, leaving aside research on supply chain problems; therefore, without economics and sufficient funding, scientific advances are not possible. In addition, industry and individual companies may also be affected by these anomalous factors that may limit the funding of useful projects to develop and deploy technologies and tools that contribute to the quality of the supply chain.
- *The lack of progress and development (R&D, in general) may benefit non-European countries to be at the forefront of this initiative:* related to the previous point, any economic repercussion affects progress and the opportunity to be at the forefront of such a proposal worldwide and remain a leader in this field.
- *Lack of interest or commitment to European digital sovereignty:* any lack of interest or ability to lead secure and trusted actions within the supply chain may have repercussions for the supply chain itself. Therefore, training and awareness are primary conditions to knowing first-hand the risks involved in the process and the importance of contributing in an appropriate and reasonable manner.

3 Recommendations

3.1 Introduction

The recommendations identified in the first report are summarised here on the basis that they have continued validity. In addition, through the rest of this section, we provide recommendations based on three sets of analyses: technological, educational and regulatory. None of these sets of recommendations could be assumed to be exhaustive, particularly the technology section; however, each of them are valid within the defined scope and could certainly claim to be indicative of broader trends.

The audiences for each of these recommendations are varied, although it is reasonable to assert that each has cogency for the major and minor actors in most supply chain settings. For example:

- the regulatory section should be of value to European policy makers and regulators as well as software vendors;

- the training section should benefit developers and implementors of educational programmes around both supply chain security and SME cybersecurity awareness;
- the technology section should provide pragmatics insights, both positive and negative about the operational deployment of blockchain, in supply chain and beyond.

3.2 Review of previous recommendations

In the first report in this series, we produced a comprehensive set of recommendations which we will review to see whether they have been adopted, or whether they should be revised/updated. In the most part however, it is not apparent they have been widely adopted and there is not an overwhelming rationale to revise or update them.

3.2.1 General IT security recommendations

This series of recommendations are more in the nature of advice and preventative good practice in general, with reference to supply chain and the implementation challenges facing SMEs. The recommendations draw on work carried out in WP4 and especially in T9.4 on SME awareness, as well as a set of recommendations and guidelines provided by ENISA.

- Adopt appropriate **risk management and incident management strategies**
- **Identify and categorise cyber assets** (infrastructures assets and data) that are critical and need protection. Then define privileged access to the assets and assign permissions and rights depending on a user's roles/tasks/attributes.
- **Make specific service-level agreements** on security with other entities in the supply chain and/or require continuous certification - and audit their compliance.
- **Make sure users/employees use unique, strong credentials**, preferably together with multifactor authentication based on written policies, frequent training and education.
- **Promote and incorporate privacy and security by design** for a secure development process for both network and systems.
- **Check out recommendations and guidelines** from other organisations, such as ENISA.
- Perform regular independent reviews and audits.

Further basic IT protection concept can potentially contribute to reducing cybersecurity costs.

- Carry out a **security threat and risk assessment** to identify the most critical digital assets in the organisation, prioritise the remaining digital assets and accordingly set cybersecurity controls for them.
- **Assess data collected** in the name of security whether it enables a better investigation or not and decide whether to collect it.
- **Focus on educating and training employees** as well as process improvement, eliminating duplicate tools and investing only in necessary technology solutions and considering single vendor solutions (if possible) which may contribute to reducing cybersecurity costs.
- **Utilise open source** cybersecurity tools as well as training and awareness resources, available for free or at a nominal cost.

3.2.2 Legal recommendations

This section explored the new features incorporated into the revision of the NIS Directive (NIS2) that was part of the Commission's 2020 Cybersecurity Strategy.

It identified the risk-management approach adopted by NIS2, which provides a list of basic security requirements and incident reporting obligations that must be applied by entities in the sectors to which they apply across the EU. It introduces more precise provisions on the process for incident reporting, including the content of reports and timelines. Among the significant changes being made are widening the scope of the law's application to additional industry sectors, strengthening the existing rules on security requirements and incident reporting, while also increasing the maximum fines that can be applied.

Amongst the proposed changes, the key sections impacting supply chains are under Chapter IV 'Cybersecurity risk management and reporting obligations' and Articles 18 and 19 in particular.

- **Article 18**, Cybersecurity risk management measures, asserts that shall ensure a level of security of network and information systems appropriate to the risk presented. And specifically, supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services.
- **Article 19**, EU coordinated risk assessments of critical supply chains by the Cooperation Group together with the Commission and ENISA.

NIS2 requires individual companies to address cybersecurity risks in supply chains and supplier relationships, emphasising supply chain risk management, demanding that the regulated entities assess the quality and the cybersecurity practices of their suppliers and service providers, especially big data companies and managed service providers, during their continued business relationship.

SMEs are recommended to comply with the NIS directive by implementing a sector-specific cyber resilience programme, not least because EU legislation has been found to have positive effects on a wide range of SMEs except for its compliance costs which again tend to diminish as SMEs become more familiar with requirements.

An up to date analysis of legislation and policy relevant to supply chains is available in section 3.4 of this report.

3.2.3 *Standards recommendations*

Here we identified a series of standards from the International Organisation for Standardisation (ISO)/ International Electrotechnical Commission (IEC) standards that target supply chain security.

Obtaining standards certification can be initially expensive (though this cost is influenced by the size and complexity of the organisations), but in the long run, it brings many benefits to most organisations, including SMEs, reducing costs, increasing productivity, and accessing new markets. For SMEs, it helps, for example, to build customer confidence, meet regulatory requirements, reduce costs, gain market access [ISO], improve innovative capacity, and enhance competitiveness [EC].

Small Business Standards (SBS), the European DIGITAL SME Alliance and others help with the standardisation efforts of the European SMEs. The SBS represents the interests of SMEs in the standardisation processes, raises SME awareness about standardisation, facilitates their uptake of standards and motivates them to engage in the standardisation processes [SBS]. Similarly, the European DIGITAL SME Alliance develops and promotes guides for the implementation of standards; for example, it developed the SME guide for the implementation of ISO/IEC 27001 on information security management [Bieliauskaite2018].

Organisations are making use of standards to build robust supply chains and to protect them from harm. If possible, it is suggested to consider using open, non-proprietary standards and certification programs.

3.2.4 *Security recommendations derived from CyberSec4Europe work*

3.2.4.1 *Recommendations from WP4*

WP4 highlights two critical issues:

- the need to adapt the emerging technologies (IT-OT) for the supply chain and to mitigate the risks and threats they introduce; and
- the threats are increasing significantly in number and severity

It goes on to identify four approaches to address these issues

(1) **Mitigations** to:

- Establish a dynamic risk assessment on the supplier side.
- Add protection at all levels and authentication.
- Propose reliable and dynamic event management mechanisms, prevention, and detection.
- Include assurance measures through verification and compliance with regulatory frameworks.
- Establish standardisation and certification measures.
- Make sure trustworthiness and resilience of operations and services are in acceptable states and at all times.
- Keep operational performance and establish measures that help control the complexity of the system to incorporate security measures and ensure the availability of processes, resources and data streams when they are demanded.
- Extend the technological and security culture within the supply chain operations.
- Establish trust between suppliers and customers.

(2) Supply chains to have the following **capabilities**:

- Traceability, procurement, and accountability
- Notification and multi- language management
- Governance and assurance
- Standardisation and certification
- Resilience
- Cyber crisis management
- Suitable hardware update
- Post-quantum cryptography
- Defensive tools

(3) **Non-technical measures** to:

- Define applicable policies and standards
- Implement standardisation and certification for new technologies that are being adopted
- Embed redundant mechanism in integrated safety systems
- Utilise and implement freely available tools
- Promote security awareness through reliable education and training programmes.

(4) **Implementing technologies** to support the above using:

- DLT for auditing and accountability mechanism allowing to establish responsibilities and transparency in the entire value chain,
- Homomorphic cryptography for the option to perform computations on encrypted data
- Strong authentication using cryptographic-based advanced methods and authorisation systems using the principle of least privilege,
- Big data, ML and AI to extract pattern and identify abnormal behaviours,
- IoT applied to the area where standards and certification are not fully developed
- Lightweight formal techniques to ensure or prove a software obtained from other developers is secure against potential attacks.

Not all these recommendations can be adopted by resource-constrained SMEs, due to lack of access expertise or unaffordability.

3.2.5.2 Recommendations from WP5

The recommendation to use DLT mentioned above was followed by the experience from WP5 which demonstrated how a permissioned blockchain can be sought to streamline the supply chain processes and stakeholder activities and address security and privacy challenges that may arise in the supply chain due to the implementation of emerging technologies and IT/OT convergence. The considered two use case demonstrators were (1) supply chain for retail (SCH-UC1), and (2) compliance and accountability in distributed manufacturing (SCH-UC2).

From an SME perspective, the challenges to the supply chain identified are equally applicable to SMEs' supply chain involvement. In addition, there are also other challenges to the diffusion of blockchain technology among SMEs, for example, low awareness of salient features of blockchain, and lack of access to digital infrastructures. Unless these challenges are addressed, a broader adoption of blockchain technology by SMEs will remain uncertain.

A full set of more recent recommendations from WP5 are covered in section 3.2.2 of this report

3.2.5 Tools recommendations

Organisations and SMEs in particular are recommended to benefit from tools and technologies that are open source and available free to use or for a nominal cost, if possible.

3.2.5.1 General available tools

A few examples of tools resulting from a simple online search covered the following areas. The first four are useful for protecting IT/OT infrastructures and networks, and employees against common attacks like phishing, malware attacks, and data breaches. The remaining tools can be used for penetrating testing and software analysis:

- Networking and operating system hardening
- Internet security
- Email security
- Password management, recovery, and attack tools
- Vulnerability scanning tools
- Networking and security auditing tools
- Cybersecurity framework and operating systems

The WP4 presented a 12-month plan to apply or adapt such security tools for supply chain security.

3.2.5.2 Tools from EU projects

Various EU projects offer free cybersecurity tools which are mainly cybersecurity self-assessment tools for organisations, particularly focusing on SMEs. Such tools are helpful to identify and learn about cyber risks, exploits and vulnerabilities in an organisation.

The projects mentioned were cyberwatching.eu, SMESEC, GEIGER and (of course) CyberSec4Europe with the caveat to assess its usefulness, the quality of documentation, the implementation complexity and expertise needed, at what phase it is in the open-source life cycle and an active feedback community.

Section 3.3 of this report looks at matters relating to operational controls and training.

3.2.6 Recommendations to the EU

The recommendations targeted to EU-funded research projects investigating cybersecurity for supply chain and their SMEs participants. The recommended approaches were:

- Risk management methodologies and frameworks
- Distributed detection, continuous monitoring and incident management
- Traceability, shared data spaces
- Privacy preservation in blockchain
- Password-less authentication
- Unlinkability and minimal disclosure

A full analysis of EU regulations, and consequent recommendations, with a potential impact on supply chains, and SMEs in particular, are covered in section 3.4 of this report. In addition, CyberSec4Europe is producing a set of two-page policy recommendation briefs, which include some of the approaches listed above.

3.2 Technology

3.2.1 What opportunities are seen for supply chain security

Supply chains have recently been under a lot of stress, and their security, resilience and robustness have become much more relevant than they were just a few years ago. There are many opportunities to improve the cybersecurity of supply chains. The most basic one is, as is almost always the case with cybersecurity, spreading awareness and employee education. While this does not necessarily improve the security itself, it does reduce mistakes and improves the effectiveness of incident responses.

There are a number of solution candidates for addressing these opportunities

- **Internet of Things (IoT) devices** are extremely useful in supply chains. A benefit of IoT is the visibility of goods from manufacturing and warehousing to distribution. Other benefits include inventory control, real-time tracking of goods, improved customer service, improved demand forecasting etc. The use of IoT in the supply chain is, therefore, high, and it will increase in the future. Unfortunately, IoT devices are also a good target for cyber attacks because their limitations can increase their vulnerability. Therefore, as the number of IoT devices in supply chains grows, the security risk to the organisations using them will increase. Securing IoT networks and devices in supply chains is an important challenge and opportunity for the future.

- With the digitalisation of supply chains, there are also large opportunities for the introduction of **better trust, traceability and transparency**. Modern customers want to know the provenance of goods, as well as being assured of their authenticity and ethical sourcing. For that, traceability throughout the entire chain must be established in a trustworthy way (so it cannot be faked) and in a way that can be easily monitored. Of course, this also fuels trust within the supply chain and adds value to the resulting products.
- **Cyber supply chain risk management (C-SCRM)** is a process designed to identify, assess and overcome risks introduced into an organisation by its supply chain. C-SCRM requires a very good security overview of an organisation, but what is generally a more significant challenge is the required security overview of third parties involved in the organisation's supply chains. With deepened interdependencies between organisations and third parties, the need for and the difficulty of assessing, improving, monitoring and managing risks throughout the lifetime of the relationship grows. This is a monumentally difficult job. The United States of America's NIST (National Institute of Standards and Technology) has created a framework¹ for helping organisations establish cybersecurity supply chain risk management, but there are large opportunities for improving C-SCRM in the future. C-SCRM can also feed off the established trust mentioned before, whereby an organisation can be assured its suppliers do not expose it to unnecessary risks, at least not in the elements that are part of the mutual trust. C-SCRM also extends to software, where establishing a chain of dependencies can be especially challenging as projects use code and solutions from other projects, for which it is hard to know if they are or will become liabilities. This requires collaboration on a large scale. For instance, Google faces similar challenges and has just launched the GUAC (Graph for Understanding Artifact Composition) project².

While there is no one solution to resolve the challenges faced by cybersecurity in supply chains, some emerging technologies show promise to be able to address (at least partially) many of the opportunities for future improvements in supply chain cybersecurity.

- **Artificial intelligence (AI)** and its subset, machine learning, are technologies that are currently discussed a lot. While the technologies have had their ups and downs in the past, there is now a lot of buzz surrounding using artificial intelligence and machine learning for cybersecurity, including cybersecurity for supply chains. While AI in managing the logistics and supply chains (demand forecasting, inventory management, automating processes using robots, chatbots for enhanced customer support, AI-supported risk analysis, transit monitoring with AI-powered IoT, autonomous vehicles for secure shipping etc.) has advanced considerably, AI for the purpose of cybersecurity is largely still an untapped resource³. Because of how versatile AI can be, it can be applied in various ways. AI can use pattern recognition and data collection to continually look for anomalous activity and identify anything mischievous rapidly. This can be applied to protect IoT networks, when attacks are using a supplier's (or third party's) access to an organisation's network to recognise untypical behaviour. AI is a good candidate to support supply chain security because it can work well with multidimensional data from dynamic situations that might be found in supply chains under attack.

¹ <https://csrc.nist.gov/News/2022/c-scrm-guidance-nist-sp-800-161r1>

² <https://security.googleblog.com/2022/10/announcing-guac-great-pairing-with-slsa.html>

³ <https://ieeexplore.ieee.org/document/9203862>

- The second very popular technology interesting for supply chains is **blockchain**. Blockchain is a type of distributed ledger technology that stores data in a way so that the data cannot be altered or removed retroactively. Also blockchains need not depend on a trustworthy third party. The main benefits the blockchain can bring to organisations are related to *trust, traceability and transparency* (see above); however, the benefits do also reach operational aspects (e.g., reducing time delays, minimising costs, and/or reducing administrative processes). Blockchains can be used in regulatory monitoring, auditing, securing and realising compliance requirements, contractual bids and agreements, product traceability and supplier payments. Data in blockchain can easily be made available, bolstering cooperation between vendors and tracking items from a source, through the supply chain, to the customer (for such purposes, it can be combined with IoT for the best results). It can also be used in software supply chains to control patching and configuration (e.g., blockchain-based patch management, blockchain-based configuration management).
- The concept of **digital twins** is fairly new. It provides a virtual representation (i.e., equivalent / “*identical*” digital counterpart) of a physical system. Generally, it is used for simulation, optimisation, integration, testing, monitoring and/or maintenance; however, it has the potential to improve security as well. Digital twins allow for security analysis and monitoring that could not be possible on a physical system, which results in better and more easily available security assessments. By simulating security attacks and, just through better visibility of system components and working processes, digital twins can prevent cyber attacks and/or show potential vulnerabilities of the system. Performing stress tests and other security tests in a digital twin also allows for much more aggressive testing without fear of compromising an organisation’s operations. Digital twins are also useful as patch management tools, where they can serve as a testing bed (without impacting the deployed infrastructure) to see any unforeseen consequences patching might have on the security and stability of the system. The same is true for any new installations to the system.

3.2.2 Evaluation / Results gained from project

WP 5 (Application demonstration use cases) evaluated technologies of which several have also been developed by partners in WP3 (Blueprint design and common research). Task 5.2, Supply chain security assurance, focused on evaluating trust technologies that allow managing cross-organisational business processes. In contrast to traditional systems where cooperation is typically set up bilaterally (e.g., between suppliers and manufacturers) and/or relies on facilitating agencies, we evaluated distributed ledger technologies – in particular blockchain – with the goal of coming up with system architectures that allow building up trust without the need for a trusted third party.

3.2.2.1 Testing and evaluating new technologies on the basis of concrete use cases

Supply chains represent cross-organisational, distributed business processes which involve various stakeholders such as manufacturers, suppliers (and sub-suppliers) and customers. In addition, authorities might be engaged as well, in order to check and control the conformance of supply chain executions with legal regulations and to provide support in case of conflicts [CS4ED54] (section 4.3).

For supply chains to work reliably, trust needs to be established and maintained between the collaborating partners. As highlighted in [CS4ED54], supply chain actors need to be able to keep control of goods and data they are exchanging. When handling data – such as technical documentation or tender documents – the flow of information needs to be controlled and confidentiality and integrity of data needs to be preserved. For instance, potential competitors must not get access to technical specifications

or price information as this could cause severe damage to a company’s business. Furthermore, the actions of participants must be traceable, and it should not be possible for them to be denied. In other words, auditability and non-repudiation are additional key concerns of secure supply chain workflows.

Therefore, Cybersec4Europe decided to evaluate distributed ledger technology with the following objectives:

- a. to determine how trust relationships between supply chain partners can be established and maintained in a dynamic ecosystem such as supply chains,
- b. to come up with solution blueprints to ensure integrity and confidentiality of data, and
- c. to determine and evaluate means for enforcing workflow compliance and accountability for cross-organisational supply chain use cases.

Overall, the developed blockchain-backed solution architectures were intended to ease digitisation of supply chains. That is, to get rid of paper-based processes wherever possible and to automate steps in distributed workflows without a trusted third party as much as possible.

As part of T5.2 Supply chain security assurance, two use case demonstrators were developed, namely:

- *SCH-UC1: Dispute resolution for retail supply chain*

This use case models supply chains for retail business. The demonstrator particularly focuses on dispute resolution: two parties may initiate a dispute whenever inconsistencies between the order of goods and the received shipments occur. Usually, dispute management implies significant costs for a company. The demonstrator shows that leveraging the blockchain to manage the supply chain’s processes can bring considerable advantages to dispute management, such as (automated) identification of root causes and the implementation of procedures via so-called smart contracts to resolve such situations. The diagram below highlights the flow of interaction when goods are delivered versus when disputes need to be identified and resolved.

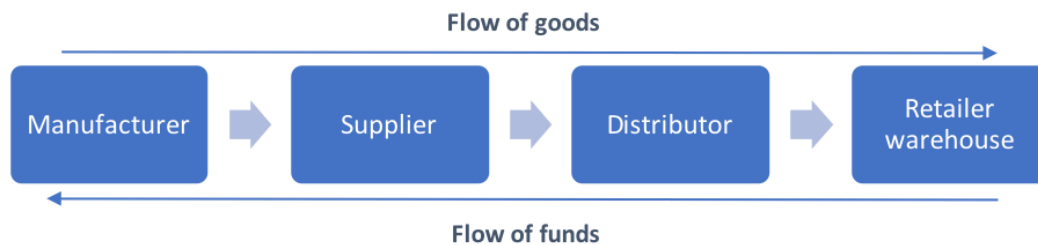


Figure 1: flow of goods and funds

Details on the architecture and the implementation of the use case demonstrator are provided in section 3.1.3 of [CS4ED55]. The asset “Blockchain Platform” developed in WP3 provides the technological basis for the demonstrator which uses a unique satellite chain architecture, where the business data is only visible to participants within each satellite chain. This ensures transaction confidentiality (see [CS4ED55] section 3.2.2.2).

Without having such a platform in place, if there is a delay or error in the shipment, the retailer raises a dispute and a significant amount of time is spent on review, evidence data collection, negotiation, and settlement. In contrast, using a blockchain-based infrastructure to establish and manage trust, the nodes of the various participants are synchronised in real-time and there is

consensus on the state of the supply chain transaction. Accordingly, data relevant for root cause analysis is available and processes for the evaluation and settlement of disputes can be automated to a large extent. As all participants have the same view of the status of deliveries and transactions, participants can (1) recognise delays faster and take remedial action without raising a dispute; and (2) if there is a dispute, then the process of review, evidence collection, negotiation and settlement is accelerated significantly. Because of this, disputes are resolved faster, and capital previously tied up in protracted legal disputes can be freed up.

- *SCH-UC2: Compliance and accountability in distributed manufacturing*

This use case focuses on scenarios where large manufacturers produce goods via distributed and rather complex processes and must track quality and compliance parameters. Compliance in manufacturing refers to technical, legal and corporate requirements, and must observe regulations and industry standards. This may involve multiple jurisdictions and supervisory bodies. Compliance must be ensured and may need to be proven not only by manufacturers, but also for instance by sub-contractors and suppliers. Thus, suppliers are required to collect design, manufacturing and test data, and to share those with authorities and their customers to prove compliance.

In [CS4ED54], a concrete manufacturing scenario of the construction of an electrical station or substation was introduced. In the given supply chain scenario, compliance denotes, for instance, the adherence to process steps and part specifications, thus, determining the overall quality of the produced goods. In the centre of our considerations, there is a large industrial manufacturing enterprise. The manufacturer designs, installs and delivers custom-built complete electrical stations or substations, for instance, with the purpose of enabling a high-voltage electrical current transmission with minimum losses. Among the main components in those stations are power transformers which might take up to one or two years to design and build. Any malfunction of such components, which could require their replacement, may imply the unavailability of the electricity grid in the affected region for months or even years. The equipment must be resilient to geomagnetic disturbances, electromagnetic pulses, severe weather, floods, etc. Concerning cybersecurity, they must be built applying secure development processes, making sure that state-of-the-art security mechanisms (e.g., concerning authentication and authorisation) are implemented and that they do not contain any malware or logic bombs (which could be implanted as part of complex cyber attacks).

As both use case address different domains – one retail business and the other project business – they complement each other very well and serve to cover the requirements introduced at the beginning. At the same time, they are based on a common architectural basis as illustrated in the diagram in Figure 2 below, which illustrates the software architecture of SCH-UC2 (see also [Kasinathan2021]).

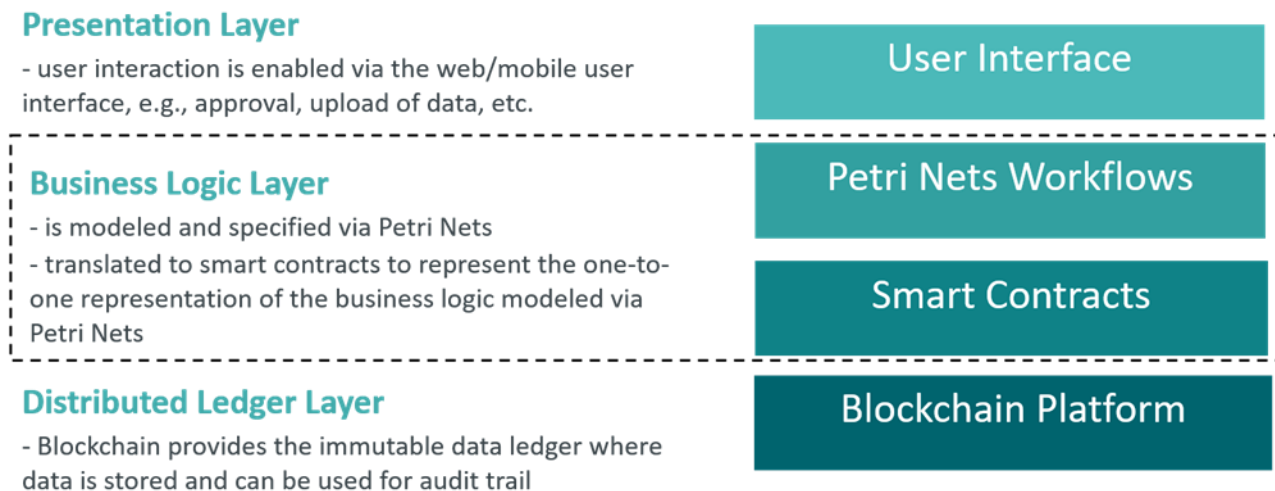


Figure 2: SCH-UC2 software architecture

The layers of the architecture are given by:

- **Presentation layer:** The user interface is designed to be modular and uses a web application framework.
- **Business logic layer:** This layer realises the business logic and is implemented by means of two components. For modelling and implementing the distributed business logic, we use **Petri nets** to create one or more **workflows** and verify them for properties such as deadlock-freeness and soundness properties. As illustrated in section 3.2.2 of [CS4ED55], Petri nets are easy to understand and can be used to trace the steps that have been completed and the required next steps in a workflow. Furthermore, there is also the possibility to automate the generation of the business logic by translating Petri nets into smart contract blueprints – which represents the second component of the business logic layer. We use **smart contracts** as a one-to-one mapping for the Petri nets-based workflow specifications, such that they act as the code that interacts with the underlying blockchain platform. A middleware is introduced to connect the Petri nets abstraction layer and the smart contracts.
- **Distributed ledger:** The introduced use cases are required to trace different entities and to hold them accountable for actions they committed within the workflow. Also, the entities involved may not want to share details of the business logic which is executed locally (such as a design phase) with other competing parties. Therefore, a permissioned distributed ledger is used to restrict access to the business logic and its related transactions. We built the implementation of our use case demonstrators on Hyperledger Fabric (HLF) 2.2 LTS⁴.

3.2.2.2 Evaluation results

To address the security requirements and challenges of complex supply chains, WP4, amongst others, recommended evaluating emerging technologies such as distributed ledger technologies (DLT) and in particular blockchain (see sections 2.1.3 and 3.2.4.1) as they bring with them good prerequisites for the realisation of auditing and accountability mechanisms. WP5 picked up on this with the implementation of blockchain-based solution architectures to realise two concrete supply chain use cases – one for retail and one for project business as presented in the previous section. The final evaluation of the requirements for the use cases SCH-UC1 and SCH-UC2 as presented in deliverable [CS4ED56] provides evidence for

⁴ <https://www.hyperledger.org/blog/2020/07/20/new-release-hyperledger-fabric-2-2-lts>

the achievability of the initially set goals for the demonstrator (see [CS4ED54]). Mandatory requirements – security as well as functional and operational ones – were addressed and validated successfully. Based on the demonstrator’s evaluation, we can conclude that the developed solution blueprints are well suited to protect against supply chain security threats that got introduced in [section 2.1.1](#) above:

- *Protection against cyber physical attacks:* With the security requirements defined in [CS4ED51] and refined in [CS4ED54], a focus was placed on the secure implementation of the demonstrator. This covered security dimensions such as authentication and authorisation, logging and auditing, as well as infrastructure security (e.g., having monitoring and incident detection mechanisms in place) and corresponding security best practices. Though the implementation of the use cases were used for the demonstration of proof-of-concept, they represent solid blueprints for a potential later integration in productive environments. We paid particular attention to the realisation of logging and auditing mechanisms. Hereby, blockchain technology (specifically, Hyperledger Fabric (HLF) LTS 2.2) was used to track and trace any user interaction with the business logic layer in a way that actions are recorded immutably in the underlying distributed ledger. Hence, non-repudiation is achieved which serves as a key building block for the identification of root causes of conflicts and subsequent dispute resolution.
- *Protection against data breaches:* Protecting corporate proprietary information in a distributed system such as supply chains is essential. When using a system architecture that is based on distributed ledgers, it is of key relevance to evaluate which information can be stored in the ledger (and which would therewith be accessible by all partners having access to the ledger) or needs to be stored and processed off-chain. It also needs to be considered that information cannot be changed or removed once it has been written to the ledger.

WP5 T5.2 had a closer look at these security and usability requirements. Both use cases had user stories concerning data that cannot be shared with all partners of a consortium. We evaluated techniques for selective data sharing and disclosure in blockchain environments, making use of Hyperledger Fabric’s channel concept as well as satellite channels offered by the “Blockchain Platform” that was developed as part of WP3. A channel “is like a virtual blockchain network that sits on top of a physical blockchain network with its own access rules” [Androulaki2018]. That way, a channel represents a segmentation of the group of participants. If selected partners want to exchange confidential information, they can set up a dedicated channel only they can use. A channel is therefore a logical communication pathway between a set of organisations that must all agree to join the channel and must authenticate themselves and their members. Additionally, each channel has its own private ledger whose read/write access rights are granted only to the channel’s members. Nodes, in turn, by joining the channel agree to share and manage identical copies of the channel’s ledger. Naturally, a single node can be a member of one or more channels at a time.

Furthermore, we evaluated how to store information that should not be made accessible to all partners off-chain by means of so-called private data collections (PDC). Data that shall only be accessible for a smaller group of nodes – restricted via HLF policies – is exchanged in private communications (i.e., via peer-to-peer communication). The peers knowing the confidential data, store it off-chain, i.e., in private state databases. Only a hash of the confidential data will be endorsed and made visible in the blockchain. That means, private data gets stored and is updated alongside the ledger while only hashes and references to that data get committed: *“The hash serves as evidence of the transaction, is used for state validation, and can be used for audit*

*purposes.*⁵ That way, private transactions building upon private data collections can also offer fine-grained access control.

Overall, we evaluated different strategies for handling confidential data securely in permissioned blockchains, using the concepts of channels and PDCs as described above. A more detailed summary of the evaluation results is provided by [Hoffmann2022].

- *Protection against impersonation attacks:* The presented solution architecture is characterized by its strength in terms of traceability of user actions. A key prerequisite for achieving non-repudiation is that actors (organisations as well as human users) can reliably be identified. This is achieved through the supported authentication means implemented for the architecture shown in **Error! Reference source not found.** and validated in [CS4ED56]. Hyperledger Fabric (HLF) builds upon public key infrastructures for managing users of the blockchain. HLF handles identity management and authentication with a combination of the traditional public key infrastructure (PKI) and a HLF component called membership service provider (MSP). The different actors in a blockchain network include peers, orderers, client applications and administrators. Each actor has an X.509 digital identity certificate and its corresponding private key. Individual X.509 certificates and their private keys and the root CA certificate chains are paired with MSPs to provide authentication against another actor within the HLF blockchain. An MSP verifies a node's certificate to prove its identity and to ensure it has the permission to do whatever action it tried based on predefined HLF policies. Organisations wanting to join the network, must establish their own PKI chain of trust structure in the form of an MSP, listing the identities of its members to the HLF network who are authorised to represent the organisation and act on its behalf within the network. To join a channel to interact with other organisations, its MSP must be included in the channel configuration, otherwise all transactions by its members will be rejected. Individuals must have a valid digital identity and must be listed as authorised members of their organization. To use existing trust bindings, it is also possible – not to say recommended best practice – to integrate the organisations' existing public key infrastructures (PKIs) and not to build up a shadow PKI for the ledger.

In addition to the threats and risks, [section 2.1.1](#) also addresses the risk of *GDPR non-compliance*. As pointed out, GDPR requirements are essential for supply chains and need to be fulfilled reliably. However, the use case demonstrators developed in T5.2 were not handling personally identifiable information (PII). That is, no user information such as user master data was collected and processed. GDPR compliance was defined as a requirement for the use cases (see [CS4ED54]) but addressed only to a limited extent because of lack of PII (see [CS4ED56]). When integrating the architectural blueprints described above into end-to-end solution architectures, PII would have to be addressed in a broader context. For instance, system components such as customer relationship management (CRM) that handle end-customer data need to be compliant with the GDPR.

3.2.2.3 Recommendations

The provided implementations and their validation demonstrate the technical feasibility of realising complex, highly distributed supply chains in a secure manner. We can conclude that blockchain-based architectures represent an appropriate technology to implement supply chain scenarios that cannot rely on a trusted third party – i.e., where it is not possible to agree on and operate a trusted third party but where partners demand for having (shared) control of the infrastructure and data. As was for instance

⁵ <https://hyperledger-fabric.readthedocs.io/en/release-2.2/private-data/private-data.html>

demonstrated by SCH-UC2's deployment, the infrastructure was realised in a way that it spans different regions and organisations.

However, we would like to point out that the realisation and operation of blockchain-based architectures is not without additional costs (compared to centrally operated systems). This refers to higher efforts due to the complexity of the overall distributed system architecture itself and regarding operational efforts, e.g., for hosting peers, orderers and clients of the HLF network. Supply chain partners must hence be able and willing to take over these additional responsibilities and must decide between the trade-off of costs for infrastructure and operation versus autonomy or independence from a trusted third party.

For SMEs this may be a barrier that prevents them from participating at this moment. To tackle this dilemma, good tool support for the definition and roll-out of blockchain-based infrastructures is needed. Therefore, we encourage **future research and development** to focus on technologies and tools for easing the definition, roll-out and verification of secure and reliable distributed architectures. The to-be developed technologies should, ideally, support the high-level process from workflow specification via automated creation and roll-out up to its verification, as illustrated in Figure 3 below. The goal would be that the (semi-) automated creation of the deployment configuration (including smart contracts, channel configuration, and private data collections) can be done based on the specification of the workflow. This would significantly contribute to reducing the overall complexity of the creation process. Additionally, tool support for the distributed deployment is needed to ease the setup of required channels, deploying the contracts and other components. Finally, tool support for the validation of correct instantiations is needed. In particular, the created blockchain network configuration must be validated with respect to the workflow specification requirements. This process is currently manual work and should be further automated with (open-source) tooling.



Figure 3: Workflow to validation

To sum up, based on the experience we have gained through our evaluation of prototypes, our recommendations are:

- (1) continuing research and development in blockchain and workflow technologies for their integration in distributed supply chain systems and to address the identified gaps.
- (2) increasing the maturity of tools and blockchain technologies (e.g., as part of open-source developments) to improve the usability of the deployed systems and thus increase industry adoption, especially among SMEs.

3.3 Organisational / training recommendations

3.3.1 Guidelines and best practices

The supply chain varies considerably from group to group and involves many different organisations in a network. This could be the reason why there is no single recognised set of supply chain cybersecurity guidelines or best practices. In fact, many countries have their own cyber supply chain guidelines.

3.3.1.1 *United Kingdom*

The UK's National Cyber Security Centre (NCSC) has proposed a set of 12 principles [NCSC2022] to assist organisations in achieving effective control and management of their supply chain security. These principles are divided into the following four stages:

- i. Understand the risks—This is an information-gathering stage in which the organisation intends to gain a comprehensive understanding of its supply chain. It contains the following three principles:
 - Understand what needs to be protected and why
 - Know who your suppliers are and build an understanding of what their security looks like
 - Understand the security risk posed by your supply chain
- ii. Establish control — this stage aids in gaining and maintaining control of the supply chain. It is comprised of the five principles listed below:
 - Communicate your view of security needs to your suppliers
 - Set and communicate minimum security requirements for your suppliers
 - Build security consideration into your contracting processes and require that your suppliers do the same
 - Meet your own security responsibilities as a supplier and consumer
 - Raise awareness of security within your supply chain
- iii. Check your management—This stage advocates for gaining confidence in the approaches used to establish control over the supply chain. It contains the following principle:
 - Build assurance activities into your supply chain management
- iv. Continuous improvement—This stage recommends that security be improved and maintained as the supply chain evolves. It includes the following two principles:
 - Encourage the continuous improvement of security within your supply chain
 - Build trust with suppliers

3.3.1.2 *Belgium*

The Belgian Centre for Cyber Security [CCSB2020] provides guidelines for information security (mainly confidentiality, integrity, and availability of assets and services) within the supply chain of network assets and services for operators of essential services (OESs). The recommendations from various standards (namely, ISO/IEC 27000, 27001, 27002, 27005, 27017, 27036, 28000, 15408, 20243:2015) and other guidelines (namely, NIST SP800-161, NIST Cybersecurity Framework Version 1.1, Baseline Information Security Guidelines — CCB edition 2019) were utilised in the guidelines. The guidelines cover

- risk management (i.e., identifying and analysing risks within the organisation related to the supply chain of network assets and services),
- security management and architecture (i.e., general management of information security for network assets and services, as well as security architecture of network assets and services),
- procurement (i.e., management of supplier relationship and procurement of network assets and services from delivery to storage),

- operational management (i.e., management and maintenance responsibilities performed by third-party, as well as services purchased from a service provider)
- incident recovery and major changes (i.e., emergency interventions on network assets and services, as well as network assets modification and replacement), and
- secure disposal (i.e., decommissioning equipment and shutting down or transitioning services).

3.3.1.3 NIST

The National Institute of Standards and Technology [NIST21] has one of the most comprehensive and widely publicised set of guidelines for cybersecurity supply chain risk management (C-SCRM), which help in identifying, assessing and mitigating cybersecurity risks throughout the supply chains at all levels of organisations. The guidelines offered are based on the cybersecurity practices and standards promoted in past NIST publications; nonetheless, they have been adapted for use in cybersecurity supply chain risk management in the current environment. NIST's detailed guidelines for C-SCRM address primarily the integration of C-SCRM into the enterprise-wide risk management processes (i.e., assessing the risks, responding to the risks and monitoring the risks), as well as requisite enterprise processes and capabilities (i.e., critical success factors) for an enterprise's successful implementation of C-SCRM. For C-SCRM integration, the report lists out

- the general cybersecurity risks throughout supply chains, and
- risk management strategies at all levels of an enterprise (i.e., enterprise, mission & business processes, and operational).

The report identifies as the critical success factors:

- C-SCRM in the acquisition life cycle, contractual agreements, and contract management,
- building effective information-sharing processes and activities into C-SCRM programmes,
- training and awareness for all individuals within the enterprise who contribute to the success of C-SCRM,
- achieving a base level of maturity in key C-SCRM key practices; measuring and managing the effectiveness of C-SCRM programmes, and
- dedicated funds and resources for the C-SCRM programmes.

3.3.1.4 ENISA

Although not a proper guideline, the report on the threat landscape for supply chains by the European Union Agency for Cybersecurity [ENISA21] contains recommendations for supply chain cybersecurity. In addition, the report also analyses a number of recent supply chain incidents and provides the taxonomy as well as the life cycle of supply chain attacks. Since supply chain attacks leverage the interconnectedness of global markets, the report highly emphasises protection and resilience against attacks that target suppliers. Moreover, the ENISA's apprehension about cyber risks stemming from third-party vulnerabilities is confirmed by its investigation, which found that 66% of supply chain attacks reported to ENISA used the supplier software or code to infiltrate and impact customer organisations. As a result, one of the primary recommendations from ENISA to every organisation is to validate third-party code and software before utilising it to ensure it has not been tampered with or manipulated. Furthermore, ENISA makes recommendations both for customers and suppliers of the supply chain that cover:

- for customers:
 - managing supply chain cybersecurity risks, and

- managing the relationship with suppliers.
- for suppliers:
 - ensuring the secure development of products and services, and
 - implementing good practices for vulnerability management.

Further, NIST has issued more extensive guidelines for software customers and vendors on defending against software supply chain attacks [NIST21]. In addition to giving an overview of software supply chain risks, this report describes how C-SCRM [Boyens2022] and the secure software development framework (SSDF) [Souppaya2022] could be implemented to identify, assess and mitigate software supply chain risks.

Indeed, although there are some differences in the above-mentioned guidelines, essentially regarding the regulations they adhere to, there are also many similarities, such as the fact that they all adhere to risk management principles, cyber defence practices and regulations established by their respective government agencies. Moreover, their recommendations are nicely and succinctly covered by NIST's three principles for supply chain cybersecurity [NIST2022b], which are:

- *Build your defences on the assumption that your system will be breached* (i.e., an organisation should always prepare on premise that a breach is inevitable).
- *Cybersecurity is a people, process and knowledge problem, not just a technological problem* (i.e., an organisation should not only focus on technology failure but also highly prioritise risks due to human error).
- *Security is security* (i.e., an organisation should not discriminate between physical security and cybersecurity, both are important).

To summarise, cybersecurity in the supply chain is not limited to strengthening an enterprise's own defence but also preparing for potential risks due to vulnerabilities in other stakeholders in the network. This necessitates the active collaboration, communication and actions of all stakeholders, both inside (e.g., department, processes) and outside (e.g., suppliers, developers, system integrators, external service providers, and other ICT/OT service providers) the enterprise. Furthermore, it also requires an enterprise-wide cultural shift towards increased awareness and preparedness for the potential ramifications of cybersecurity throughout the supply chain. And to accomplish this, an enterprise should incorporate perspectives from several disciplines and processes into its approaches to managing cybersecurity risks throughout the supply chain [NIST2022b].

3.3.2 Awareness and Training

The above-mentioned recommendations and best practices make it abundantly clear that supply chain cybersecurity incorporates all three pillars of cybersecurity: people, process, and technology. Unfortunately, human employees often do not have a good reputation in organisational cybersecurity. In 2022, around 82% of data breaches contained human elements, including social attacks, errors and misuse [Verizon2022]. This is why NIST's C-SCRM guidelines place a heavy emphasis on cybersecurity awareness and training for individuals throughout the supply chain. Many national agencies, projects and private organisations offer awareness and training on cyber supply chains.

3.3.2.1 BSI

The British Standards Institution [BSI2022] offers many sorts of supply chain security awareness and training to a global audience. Its training covers a wide range of supply chain security issues, including security risk management, security standards and certifications (e.g., ISO 28000, AEO), and compliance with security regulations. The training is also available in a private and customised format to meet the

demands of any particular company. In general, the training covers security issues such as threat identification and reporting, access control management, policy and procedures development and implementation, application of risk management best practices, implementation of important supplier auditing, compliance with security regulations and meeting the requirements and specifications of international standards and certifications.

3.3.2.2 *NICCS*

The National Initiative for Cybersecurity Career and Studies (NICCS) from Cybersecurity and Infrastructure Security Agency [CISA2022] offers a basic course on “Cyber Supply Chain Risk Management.” In general, the course teaches learners how to securely provision, analyse, oversee and govern, protect and defend a supply chain. More specifically, it covers diversified topics such as:

- Identification of adversaries’ role in supply chain risk management.
- Defining risks related to supply chains.
- Principles of supply chain management.
- Identification of suitable security measures and tools, as well as their implementation for addressing supply chain vulnerabilities.
- Evaluation of products as IoT devices.
- Security risks originating from bring your own device (BYOD).
- Threats from acquisition personnel.
- Organisation’s cybersecurity.

3.3.2.3 *Horizon 2020 projects*

Then, there are some projects funded by the EU's Horizon 2020 research and innovation programme, such as Cyber MAR [CyberMAR2022] and CyberSec4Europe [Goodman2022], that employed more intuitive approaches like cyber range environment and cybersecurity exercises respectively, to train and raise awareness on cybersecurity issues and mitigations to organisation staff. Cyber MAR trains to defend against cyber concerns in the maritime logistics value chain, whereas CyberSec4Europe’s exercises focused on cybersecurity issues encountered in organisations in general. It is well acknowledged that such intuitive and practical approaches are particularly effective in improving cybersecurity knowledge, attitude, and behaviour of people over time.

3.3.2.4 *Private organisations*

Aside from the above, several private organisations, such as SANS Institute [SANS2022] and Global Learning Systems [GLSystems2022], provide supply chain security awareness and training. However, their training is only available for a fee.

3.3.2.5 *cyberwatching.eu*

Last but not the least, “Cybersecurity and Privacy Marketplace” [Cyberwatching2022] from cyberwatching.eu has consolidated a collection of outcomes, products, and services from completed EU-funded research projects. It contains hundreds of beneficial cybersecurity products and services from which organisations may benefit and thereby boost their supply chain cybersecurity.

3.4 **Regulation Analysis**

3.4.1 *Introduction*

The European Union has constantly been trying to adapt its regulations according to the most important challenges, considering current developments and future trends. This is also shown in the many packages of EU security legislation, which came in periodic intervals to cover progress made and new challenges ahead. In addition, the focus has shifted from firm security in general, focused on large companies, to integrate supply chain partners and SMEs. This section aims to assess the security regulations on how they address supply chains (SCs) and small and medium-sized enterprises (SMEs).

The investigations for this section are based on a desk study of primary and secondary literature and an exchange with supply chain and cybersecurity experts. In the first step, key legal documents are defined. Then, the relevant provisions, supply chain and SME aspects will be presented. Finally, as a result, possible gaps or shortcomings in addressing security for supply chains and SMEs are presented.

In the following, the key documents listed will be analysed for how the regulations of the EU address supply chain and SME-related aspects:

- Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (**NIS1**)
- Proposal for a directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (**NIS2**)
- Proposal for a regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (**Cyber resilience Act**)
- Regulation 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (**Cybersecurity Act**)
- Proposal for a directive on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937 (**Due Diligence**)
- Regulation (EU) 2021/887 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (**ECCC**)
- Directive (EU) 2015/2366 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (**PSD2**)
- Guideline on a Trans-European Automated Real-time Gross settlement Express Transfer system (**TARGET2**)
- Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (**eIDAS**)
- Directive 2014/53/EU on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (**RED**)
- Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**General Data Protection Regulation – GDPR**)
- Proposal for a regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (**Regulation on Privacy and Electronic Communications – ePrivacy**)

- Proposal for a regulation on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 (**DORA**)

3.4.2 Analysis per regulation

3.4.2.1 Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS1)

In August 2016, the European Parliament agreed on the Network and Information Security Directive (NIS Directive) as part of the EU's efforts to create a higher standard of cybersecurity for European organisations. Specifically, the NIS Directive aims to ensure the security of critical services and utilities and digital market industries for business continuity and the safety of citizens. The NIS Directive requires operators and service providers in vulnerable industries (energy, transport, banking and finance, healthcare, water, and digital infrastructure) to implement more stringent cybersecurity solutions to address modern and evolving cyber threats. The Directive also calls for measures to mitigate the impact of incidents, introduce new reporting procedures, and establish national committees to monitor compliance and coordinate them with other EU members. NIS1 has only minor parts that address supply chain and SMEs which are highlighted in the following boxes:

The criticality of services for the respective customers must be ascertained to determine the policy's scope.

"For the purpose of the review referred to in Article 23 and by November 9 2018, and every two years thereafter, Member States shall submit to the Commission the information necessary to enable the Commission to assess the implementation of this Directive, in particular the consistency of Member States' approaches to the identification of operators of essential services. That information shall include at least: [...] (d) thresholds, where they exist, to determine the relevant supply level by reference to the number of users relying on that service as referred to in point (a) of Article 6(1) or to the importance of that particular operator of essential services as referred to in point (f) of Article 6(1)."

If an essential service provider is dependent on a third-party digital service provider, this must be reported to that service provider.

"Where an operator of essential services relies on a third-party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified by that operator."

It is beneficial for SMEs to receive information about incidents.

"Information about incidents is increasingly valuable to the general public and businesses, particularly small and medium-sized enterprises."

The 2016 NIS Directive presents supply chain aspects and SMEs secondarily because only very few references to them were found. Even though the NIS Directive acknowledges that suppliers and third-party digital service providers fulfilling essential services must be included in the analysis for cybersecurity, a broader view of the supply chain is not in the scope of the NIS Directive. Concerning SMEs, the NIS Directive only applies to companies with more than 50 staff and an annual turnover or balance sheet above 10 MEUR. This means that small and micro-sized enterprises are excluded from the implementation of the NIS Directive, but medium-sized enterprises, in this sense, are not excluded. However, it is mentioned that information about cyber-attacks is also of interest to SMEs to prepare themselves accordingly and identify possible lateral movements through the systems.

3.4.2.2 Proposal for a directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (NIS2)

The content of the second updated Network and Information Security Directive (NIS2) was first proposed by the EC in December 2020. The content was finalised in May 2022. NIS2 aims to strengthen the the NIS Directive legal framework to consider the internal market's development and the diversification of threats. For this reason, it forces many more companies in Internet access services, data centre services, wholesale, research, postal services or waste management to apply more cybersecurity measures. Another objective is to improve cyber resilience within the EU by ensuring that critical actors are aware of these risks and have taken the necessary measures to combat them. NIS2 additionally covers the areas of crisis and incident management as well as improved organisational risk management. It also regulates encryption, security testing and management and vulnerability disclosure. Other new features of NIS2 include the obligation to report incidents (cyber-attacks, data loss, etc.) that pose significant operational or financial risks. Finally, sanctions are foreseen for companies that do not comply with organisational and technical measures. NIS2 partly addresses supply chain and SMEs and are highlighted in the following boxes:

Suppliers of ICT products need to establish processes to obtain vulnerability information from third parties.

"(28) Since the exploitation of vulnerabilities in network and information systems may cause significant disruption and harm, swiftly identifying and remedying those vulnerabilities is an important factor in reducing cybersecurity risk. Entities that develop such systems should therefore establish appropriate procedures to handle vulnerabilities when they are discovered. Since vulnerabilities are often discovered and reported (disclosed) by third parties (reporting entities), the manufacturer or provider of ICT products or services should also put in place the necessary procedures to receive vulnerability information from third parties."

Shown by various incidents, the supply chain, including the overall quality of products within the whole product development process and cybersecurity practices of their supply chain partners and the whole surrounding ecosystem, are essential when addressing cybersecurity risks.

"(43) Addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers is particularly important given the prevalence of incidents where entities have fallen victim to cyber-attacks and where malicious actors were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third party products and services. Entities should therefore assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. [...] (45) Entities should also address cybersecurity risks stemming from their interactions and relationships with other stakeholders within a broader ecosystem. In particular, entities should take appropriate measures to ensure that their cooperation with academic and research institutions takes place in line with their cybersecurity policies and follows good practices as regards secure access and dissemination of information in general and the protection of intellectual property in particular" S. 21 [...] "Member States shall ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, entities shall take into account the vulnerabilities specific to each supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures."

Supply chain risk assessments, considering technical and non-technical factors, need to be carried out to identify the critical ICT services, systems, and products, relevant threats, and vulnerabilities per sector.

"(46) To further address key supply chain risks and assist entities operating in sectors covered by this Directive to appropriately manage supply chain and supplier related cybersecurity risks, the Cooperation Group involving relevant national authorities, in cooperation with the Commission and ENISA, should carry out coordinated sectoral supply chain risk assessments, as was already done for 5G networks following Recommendation (EU) 2019/534 on Cybersecurity of 5G networks, with the aim of identifying per sector which are the critical ICT services, systems or products, relevant threats and vulnerabilities. (47) The supply chain risk assessments, in light of the features of the sector concerned, should take into account both technical and, where relevant, non-technical factors including those defined in Recommendation (EU) 2019/534, in the EU wide coordinated risk assessment of 5G networks security and in the EU Toolbox on 5G cybersecurity agreed by the Cooperation Group."

Five criteria determine the relevance of the supply chain: dependency, criticality, availability of alternatives, resilience maturity level, and future relevance.

"To identify the supply chains that should be subject to a coordinated risk assessment, the following criteria should be taken into account: (i) the extent to which essential and important entities use and rely on specific critical ICT services, systems or products; (ii) the relevance of specific critical ICT services, systems or products for performing critical or sensitive functions, including the processing of personal data; (iii) the availability of alternative ICT services, systems or products; (iv) the resilience of the overall supply chain of ICT services, systems or products against disruptive events and (v) for emerging ICT services, systems or products, their potential future significance for the entities' activities."

Micro and small entities are generally excluded from the NIS directive. However, exceptions are important entities that are relieved due to a lighter ex-post supervisory regime.

"The proposal foresees a general exclusion of micro and small entities from the NIS scope and a lighter ex-post supervisory regime applied to a large number of the new entities under the revised scope (so-called important entities). These measures aim to minimise and balance the burden put on companies and public administrations." S. 8 [...] "Micro and small entities within the meaning of Commission Recommendation 2003/361/EC of May 6 2003 are excluded from the scope of the Directive, except for providers of electronic communications networks or of publicly available electronic communications services, trust service providers, Top-level domain name (TLD) name registries and public administration, and certain other entities, such as the sole provider of a service in a Member State."

Specific criteria for micro and small enterprises will be elaborated.

"(10) The Commission, in cooperation with the Cooperation Group, may issue guidelines on the implementation of the criteria applicable to micro and small enterprises."

Further policies must be adopted to guide SMEs in improving resilience to cybersecurity threats.

"2. As part of the national cybersecurity strategy, Member States shall in particular adopt the following policies: (h) a policy addressing specific needs of SMEs, in particular those excluded

from the scope of this Directive, in relation to guidance and support in improving their resilience to cybersecurity threats."

Compared to the NIS Directive, NIS2 significantly places the supply chain in the foreground regarding cybersecurity. This means that not only companies that have to deal directly with the scope of the Directive are affected, but also the entire supply chain surrounding the company. This is also evident in the list of necessary measures, as supply chain security is one of the seven necessary measures. Starting with the direct suppliers of the so-called essential entities and important entities, supply chain cybersecurity measures must be established in the area of incident response, penetration testing and security audits.

As with the NIS Directive, NIS2 does not directly include small and micro-sized enterprises. Nevertheless, SMEs are an important part of supply chains, which is also recognised in the Directive. For this reason, the Commission has decided to provide special guidelines for SMEs so that resource-poor SMEs can also operate in accordance with NIS2 and thus ensure the security of supply chains.

3.4.2.3 Proposal for a regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act)

The Cyber Resilience Act was introduced in 2021, and the objective is to make things more secure and hold manufacturers accountable for cybersecurity throughout the lifespan of a device. It applies to all digital items whose use entails a direct or indirect logical or physical data link. In this perspective, a product with digital aspects is any software or hardware product that includes remote data processing technologies. Before and during the placement of a product with digital components on the market, economic operators covered by the CRA (particularly producers, importers and distributors of products with digital elements) must perform specific requirements regarding cyber-safe product design, the implementation of vulnerability handling processes and the technical documentation of a product. Non-compliance with the obligations incurs a fine with penalties of up to 2.5% of global annual turnover. The cyber resilience act partly addresses supply chain and SMEs and are highlighted in the following boxes:

The entire supply chain must be considered to avoid cybersecurity incidents and their consequences, such as disruptions or life-threatening events.

"In a connected environment, a cybersecurity incident in one product can affect an entire organisation or a whole supply chain, often propagating across the borders of the internal market within a matter of minutes. This can lead to severe disruption of economic and social activities or even become life threatening." S. 1 [...] "Cybersecurity of the entire supply chain is ensured only if all its components are cyber-secure."

All supply chain partners involved in the value-creation and distribution of products with digital elements underlie adequate obligations.

"Obligations would be set up for economic operators, starting from manufacturers, up to distributors and importers, in relation to the placement on the market of products with digital elements, as adequate for their role and responsibilities on the supply chain."

Identifying and documenting product components is an essential task to facilitate vulnerability analysis.

"(37) In order to facilitate vulnerability analysis, manufacturers should identify and document components contained in the products with digital elements, including by drawing up a software bill of materials. A software bill of materials can provide those who manufacture, purchase, and operate software with information that enhances their understanding of the supply chain, which has multiple benefits, most notably it helps manufacturers and users to track known newly emerged vulnerabilities and risks. It is of particular importance for manufacturers to ensure that their products do not contain vulnerable components developed by third parties."

Manufacturers shall do due diligence when installing external components in products with digital elements.

"4. manufacturers shall exercise due diligence when integrating components sourced from third parties in products with digital elements. They shall ensure that such components do not compromise the security of the product with digital elements."

Manufacturers must establish an ongoing risk assessment process for their products with digital elements, including documentation of known vulnerabilities and relevant information from third parties.

"5. The manufacturer shall systematically document, in a manner that is proportionate to the nature and the cybersecurity risks, relevant cybersecurity aspects concerning the product with digital elements, including vulnerabilities they become aware of and any relevant information provided by third parties, and, where applicable, update the risk assessment of the product"

All supply chain partners involved in the value-creation and distribution of products with digital elements underlie adequate obligations.

"Obligations would be set up for economic operators, starting from manufacturers, up to distributors and importers, in relation to the placement on the market of products with digital elements, as adequate for their role and responsibilities on the supply chain."

Identifying and documenting product components is an essential task to facilitate vulnerability analysis.

"(37) In order to facilitate vulnerability analysis, manufacturers should identify and document components contained in the products with digital elements, including by drawing up a software bill of materials. A software bill of materials can provide those who manufacture, purchase, and operate software with information that enhances their understanding of the supply chain, which has multiple benefits, most notably it helps manufacturers and users to track known newly emerged vulnerabilities and risks. It is of particular importance for manufacturers to ensure that their products do not contain vulnerable components developed by third parties."

Manufacturers shall do due diligence when installing external components in products with digital elements.

"4. manufacturers shall exercise due diligence when integrating components sourced from third parties in products with digital elements. They shall ensure that such components do not compromise the security of the product with digital elements."

Manufacturers must establish an ongoing risk assessment process for their products with digital elements, including documentation of known vulnerabilities and relevant information from third parties.

"5. The manufacturer shall systematically document, in a manner that is proportionate to the nature and the cybersecurity risks, relevant cybersecurity aspects concerning the product with digital elements, including vulnerabilities they become aware of and any relevant information provided by third parties, and, where applicable, update the risk assessment of the product."

The fee rate must consider the specific interests and needs of SMEs.

"5. Notified bodies shall take into account the specific interests and needs of small and medium sized enterprises (SMEs) when setting the fees for conformity assessment procedures and reduce those fees proportionately to their specific interests and needs."

The Cyber Resilience Act signifies a great improvement in transparency in the supply chain of digital products. While it has been difficult in the past and is still difficult today to understand to which extent one's own company or organisation is affected by a cyber-attack, this problem is to be solved significantly by the Cyber Resilience Act. Accordingly, the supply chain plays a central role in the Cyber Resilience Act, which will enable companies in the future to determine their own vulnerability in the event of a supply chain cyber-attack and to be able to implement resilience measures in advance to limit their vulnerability accordingly. If SMEs are now considered, they are as much a part of this legislation as large companies. Only the amount of the penalties in the current version of the Cyber Resilience Act considers the resources of SMEs.

3.4.2.4 Regulation 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

The European Cyber Security Act (the "Cybersecurity Act") went into force on 27 June 2019. A permanent mandate for ENISA and the implementation of a harmonised European certification system for ICT goods, services and processes are key components of the law. Cybersecurity certificates issued under such a scheme shall certify that ICT products, services and processes assessed under the scheme meet the specified security requirements. A scheme may specify one or more of the trustworthiness levels 'low', 'medium', and 'high' for ICT products, services and processes. In the case of low risk corresponding to the trustworthiness level "low", a self-assessment of conformity may also be provided for. Vertical needs for sectors or applications and horizontal requirements for specific technologies, such as WLAN connectivity, can be stated. The Cybersecurity Act partly addresses supply chain and SMEs and are highlighted in the following boxes:

Providing information through cooperation with universities and scientific institutions should reduce dependence on non-European cybersecurity products and strengthen supply chains within the EU.

"(4) By making the relevant information available to the public, the European Union Agency for Network and Information Security (ENISA), as established by Regulation (EU) No 526/2013 of the European Parliament and of the Council (5) contributes to the development of the cybersecurity industry in the Union, in particular SMEs and start-ups. ENISA should strive for closer cooperation with universities and research entities in order to contribute to reducing dependence on cybersecurity products and services from outside the Union and to reinforce supply chains inside the Union."

ICT products and systems include third-party technologies and components that create additional cybersecurity risks due to dependency. These dependencies need to be identified and documented by the end-user to improve cybersecurity risk management.

"(11) Modern ICT products and systems often integrate and rely on one or more third-party technologies and components such as software modules, libraries or application programming interfaces. This reliance, which is referred to as a 'dependency', could pose additional cybersecurity risks as vulnerabilities found in third-party components could also affect the security of the ICT products, ICT services and ICT processes. In many cases, identifying and documenting such dependencies enables end users of ICT products, ICT services and ICT processes to improve their cybersecurity risk management activities by improving, for example, users' cybersecurity vulnerability management and remediation procedures."

Global ICT supply chains require mutual recognition of European cybersecurity certificates. For this reason, specific conditions for mutual recognition with third countries will be developed.

"(105) In order to further facilitate trade, and recognising that ICT supply chains are global, mutual recognition agreements concerning European cybersecurity certificates may be concluded by the Union in accordance with Article 218 of the Treaty on the Functioning of the European Union (TFEU). The Commission, taking into account the advice from ENISA and the European Cybersecurity Certification Group, may recommend the opening of relevant negotiations. Each European cybersecurity certification scheme should provide specific conditions for such mutual recognition agreements with third countries."

SMEs are relevant stakeholders and, therefore, should be represented in the stakeholder cybersecurity certification group.

"(62) The Stakeholder Cybersecurity Certification Group should be established in order to help ENISA and the Commission facilitate the consultation of relevant stakeholders. The Stakeholder Cybersecurity Certification Group should be composed of members representing industry in balanced proportions, both on the demand side and the supply side of ICT products and ICT services, and including, in particular, SMEs, digital service providers, European and international standardisation bodies, national accreditation bodies, data protection supervisory authorities and conformity assessment bodies pursuant to Regulation (EC) No 765/2008 of the European Parliament and of the Council (16), and academia as well as consumer organisations."

The impact of this Directive on innovation, barriers to market entry, and costs for the end user must be assessed primarily from the point of view of SMEs.

"The Commission should evaluate the positive and negative impact of its request on the specific market in question, especially its impact on SMEs, on innovation, on barriers to entry to that market and on costs to end users." LI

The ENISA Advisory Group should include experts from relevant stakeholders, including SMEs.

"1. The Management Board, acting on a proposal from the Executive Director, shall establish in a transparent manner the ENISA Advisory Group composed of recognised experts representing the relevant stakeholders, such as the ICT industry, providers of electronic communications networks or services available to the public, SMEs, operators of essential services, consumer groups, academic experts in the field of cybersecurity, and representatives of competent authorities notified in accordance with Directive (EU) 2018/1972, of European standardisation organisations, as well as of law enforcement and data protection supervisory authorities."

When developing the terms and conditions, SMEs' interests should be considered.

L151/69 18. Conformity assessment bodies shall operate in accordance with a set of consistent, fair and reasonable terms and conditions, taking into account the interests of SMEs in relation to fees.

The Cybersecurity Act acknowledges that ICT products and the processes behind them are subject to multinational and complex supply chains that involve numerous third parties and make transparency difficult. This problem is actively addressed in the Cybersecurity Act and is one of the arguments why a uniform certification within the EU makes sense. Furthermore, the Cybersecurity Act sees this certification as an opportunity for European supply chains to compete more attractively against global products as standards are met and enforced. In terms of SMEs, the Cybersecurity Act sees SMEs as major beneficiaries of this certification, as it will ensure that secure suppliers of ICT products, services and processes can be more easily identified. However, it is undisputed that SMEs make an important contribution to this landscape and that the needs and barriers of SMEs must, therefore, also be considered.

3.4.2.5 Proposal for a directive on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937 (Due Diligence)

The EC announced a proposal for a Corporate Sustainability Due Diligence Directive on 23 February 2022, which sets due diligence criteria for both environmental and human rights problems across global value chains. The new order expands firms' responsibilities outside their own activities and provides potential victims with more legal options, offering clarity and a fair playing field. Companies are required to continuously monitor and improve their compliance performance on issues such as child labour, worker exploitation, safe and healthy working conditions, biodiversity loss and environmental pollution. Directors are held accountable for designing and overseeing due diligence procedures and implementing them into their organisations' strategies. Member States are expected to adopt appropriate consequences, including fines and compliance orders, and to compensate victims. The Due Diligence Directive partly addresses supply chain and SMEs and are highlighted in the following boxes:

Identifying and managing human rights and environmental risks in complex and global supply chains is a major challenge for many companies.

"EU companies operate in complex surroundings and, especially large ones, rely on global value chains. Given the significant number of their suppliers in the Union and in third countries and the overall complexity of value chains, EU companies, including the large ones, may encounter difficulties to identify and mitigate risks in their value chains linked to respect of human rights or environmental impacts. Identifying these adverse

impacts in value chains will become easier if more companies exercise due diligence and thus more data is available on human rights and environmental adverse impacts."

Due to their global nature, supply chains are subject to numerous regulations that differ significantly in their interpretation and the necessary measures. This Directive aims to improve this situation.

"Moreover, companies supplying goods or services, in particular SMEs, will be confronted with diverging rules and expectations from customers located in different Member States. For instance, whilst one Member State law may require the supplier to carry out third-party audits, another Member State may require the same supplier to participate in a recognised industry schemes and multi-stakeholder initiatives. One Member State may require the company to carry out due diligence in relation to established business relationships whilst the other Member State may cover the direct suppliers only. This would lead to a multiplication of different partially incompatible requirements distorting the free flow of goods and services in the Union." [...] "The proposed civil liability regime would clarify which rules apply in case harm occurs in a company's own operation, at the level of its subsidiaries and at the level of direct and indirect business relations in the value chain. In addition, the proposed provision on applicable law serves the purpose of ensuring application of the harmonised rules, including on civil liability, also in cases where otherwise the law applicable to such claim is not the law of a Member State. It will therefore be essential to ensure the necessary level-playing field."

This guideline aims to establish a horizontal framework for companies to identify, prevent, mitigate and address negative impacts on human rights and the environment in their value chain, and to put in place appropriate structures and measures to achieve this goal.

"Against this background, this Directive will set out a horizontal framework to foster the contribution of businesses operating in the single market to the respect of the human rights and environment in their own operations and through their value chains, by identifying, preventing, mitigating and accounting for their adverse human rights, and environmental impacts, and having adequate governance, management systems and measures in place to this end."

This framework is used to integrate global business processes across the entire value chain into a risk management process concerning human rights and environmental risks.

"In particular, this Directive will:

(1) improve corporate governance practices to better integrate risk management and mitigation processes of human rights and environmental risks and impacts, including those stemming from value chains, into corporate strategies;"

Due diligence measures must be implemented throughout the whole product or service life cycle, from the company's business activities at its sites and its subsidiaries to direct and indirect business relationships along the value chain.

"(15) Companies should take appropriate steps to set up and carry out due diligence measures, with respect to their own operations, their subsidiaries, as well as their established direct and indirect business relationships throughout their value chains in accordance with the provisions of this Directive. This Directive should not require

companies to guarantee, in all circumstances, that adverse impacts will never occur or that they will be stopped." [...] "In order for the due diligence to have a meaningful impact, it should cover human rights and environmental adverse impacts generated throughout the lifecycle of production and use and disposal of product or provision of services, at the level of own operations, subsidiaries and in value chains."

Quantitative and qualitative information must be regularly collected along the value chain and at special events.

"In order to allow for a comprehensive identification of adverse impacts, such identification should be based on quantitative and qualitative information. For instance, as regards adverse environmental impacts, the company should obtain information about baseline conditions at higher risk sites or facilities in value chains. Identification of adverse impacts should include assessing the human rights, and environmental context in a dynamic way and in regular intervals: prior to a new activity or relationship, prior to major decisions or changes in the operation; in response to or anticipation of changes in the operating environment; and periodically, at least every 12 months, throughout the life of an activity or relationship."

A prevention action plan needs to be established by companies, which can be implemented through contractual agreements and investments in supply chain partners such as training.

"Where necessary due to the complexity of prevention measures, companies should develop and implement a prevention action plan. Companies should seek to obtain contractual assurances from a direct partner with whom they have an established business relationship that it will ensure compliance with the code of conduct or the prevention action plan, including by seeking corresponding contractual assurances from its partners to the extent that their activities are part of the companies' value chain. The contractual assurances should be accompanied by appropriate measures to verify compliance. To ensure comprehensive prevention of actual and potential adverse impacts, companies should also make investments which aim to prevent adverse impacts, provide targeted and proportionate support for an SME with which they have an established business relationship such as financing, for example, through direct financing, low-interest loans, guarantees of continued sourcing, and assistance in securing financing, to help implement the code of conduct or prevention action plan, or technical guidance such as in the form of training, management systems upgrading, and collaborate with other companies."

Periodic assessments are to be carried out in the value chain to evaluate the effectiveness of the measures on an ongoing basis.

"(43) Companies should monitor the implementation and effectiveness of their due diligence measures. They should carry out periodic assessments of their own operations, those of their subsidiaries and, where related to the value chains of the company, those of their established business relationships, to monitor the effectiveness of the identification, prevention, minimisation, bringing to an end and mitigation of human rights and environmental adverse impacts."

SMEs are generally excluded from this Directive due to a lack of financial and administrative structures. Nevertheless, they may be affected by this Directive in their role as business partners or in high-impact sectors, for which they will receive support in the implementation.

"As regards the "personal scope" of the due diligence obligations (i.e. which business categories are covered), small and medium sized enterprises (SMEs) that include micro companies and overall account for around 99 % of all companies in the Union, are excluded from the due diligence duty. For this category of companies, the financial and administrative burden of setting up and implementing a due diligence process would be relatively high. For the most part, they do not have pre-existing due diligence mechanisms in place, they have no know-how, specialised personnel, and the cost of carrying out due diligence would impact them disproportionately. They will, however, be exposed to some of the costs and burden through business relationships with companies in scope as large companies are expected to pass on demands to their suppliers. Hence, supporting measures will be necessary to help SMEs build operational and financial capacity. Companies whose business partner is an SME, are also required to support them in fulfilling the due diligence requirements, in case such requirements would jeopardize the viability of the SME. Moreover, the value chain of the financial sector does not cover SMEs that are receiving loan, credit, financing, insurance or reinsurance. At the same time, exposure of an individual SME to adverse sustainability impacts will as a general rule be lower than the exposure of larger companies. Therefore, very large companies will be within the scope of the full due diligence obligation, also because many of them already have certain processes in place e.g. because of reporting obligations. In particular, the selected turnover criteria will filter those having the largest impact on the Union economy. Moreover, this Directive lays down measures to limit the passing on of the burden from those large companies to the smaller suppliers in the value chain and to use fair, reasonable, non-discriminatory and proportionate requirements vis-a-vis SMEs."

Standard clauses for contracts will be provided to support SMEs.

"In order to facilitate companies' compliance with their due diligence requirements through their value chain and limiting shifting compliance burden on SME business partners, the Commission should provide guidance on model contractual clauses."

SMEs are only required to identify actual and potentially serious adverse impacts relevant to their sector.

"(31) In order to avoid undue burden on the smaller companies operating in high-impact sectors which are covered by this Directive, those companies should only be obliged to identify those actual or potential severe adverse impacts that are relevant to the respective sector."

Contracts with SMEs must be fair, reasonable, and non-discriminatory. Should reviews be necessary, the costs must be borne by the non-SME.

"When contractual assurances are obtained from, or a contract is entered into, with an SME, the terms used shall be fair, reasonable and non-discriminatory. Where measures to verify compliance are carried out in relation to SMEs, the company shall bear the cost of the independent third-party verification."

In the Corporate Due Diligence Directive, the supply chain represents an essential scope for the implementation of monitoring measures and emphasises that the consideration of the entire supply chain is essential. The implementation of an end-to-end risk management process, including ongoing risk identification and monitoring processes, is the main aspect concerning the supply chain of many companies. Exceptions to this Directive are that SMEs do not have the resources to monitor the end-to-end supply chain. Nevertheless, as part of large global supply chains, they are obliged to monitor current and potentially serious risks and take measures to deal with them. For those companies, however, support is promised in several text passages, which are made available to SMEs in the form of documentation and financial facilitation.

3.4.2.6 *Regulation (EU) 2021/887 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (ECCC)*

To further enhance the cybersecurity environment, the EC and the High Representative for Foreign and Security Policy issued a Joint Communication in September 2017 to strengthen the EU's resilience, deterrence and reaction to cyber-attacks. The Communication recognised the need to retain and develop critical cybersecurity technology capabilities to protect the Digital Single Market. In this context, the proposal attempted to establish a tailor-made collaboration model in which the Competence Centre promoted and aided in coordinating the network's operations while also nurturing the cybersecurity competence community, pushing the agenda and enabling access to experts.

The Regulation partly addresses supply chain and SMEs and are highlighted in the following boxes:

Throughout the value chain of ICT products, services, and processes, as well as the development of these processes, opportunities for malicious infiltration must be minimized by enabling third parties to provide updates after the end of the service of products.

"In order to establish a sustainable cybersecurity environment, it is important that security by design is used as a principle in the process of developing, maintaining, operating and updating infrastructures, products and services, in particular by supporting state-of-the-art secure development methods, adequate security testing and security audits, by making available updates remedying known vulnerabilities or threats without delay and, where possible, by enabling third parties to create and provide updates beyond the respective end-of-service of products. Security by design should be ensured throughout the lifetime of ICT products, services or process and by the development processes that constantly evolve to reduce the risk of harm from malicious exploitation."

SMEs are important stakeholders of this guideline and should have access to the results of the competence centers to offer them the opportunity to build cyber-secure structures to remain competitive in the global market.

"Small and medium-sized enterprises (SMEs) are crucial stakeholders in the Union's cybersecurity sector and can provide cutting-edge solutions due to their agility. However, SMEs that are not specialised in cybersecurity are also prone to be more vulnerable to cybersecurity incidents due to high investment and knowledge requirements for the establishment of effective cybersecurity solutions. It is therefore necessary that the Competence Centre and the Network of National Coordination Centres (the 'Network') provide support for SMEs by facilitating the access of SMEs to knowledge and tailoring access to the results of research and development, in

order to allow SMEs to make themselves sufficiently secure and to allow SMEs that are active in cybersecurity to be competitive and contribute to the Union's leadership in the area of cybersecurity."

The further development of the ICT infrastructure should serve the industry, especially SMEs, scientific institutions, the civilian population, and the public sector.

"However, the Competence Centre should be able to facilitate the development of ICT infrastructures at the service of industries, in particular SMEs, research communities, civil society and the public sector, consistently with the mission and objectives laid down in this Regulation."

The strategic advisory board should be balanced according to the stakeholders addressed, especially concerning the representation of SMEs.

"The representation of the different stakeholders in the Strategic Advisory Group should be balanced, with particular attention paid to the representation of SMEs, in order to ensure that stakeholders are appropriately represented in the work of the Competence Centre."

One of the aims of this Directive is to strengthen the cybersecurity industry, especially SMEs, to acquire potential markets and identify development opportunities. With the help of support and technical assistance, SMEs are to be strengthened in their cybersecurity.

"... through the Agenda and the multiannual work programme, while avoiding any duplication of activities with ENISA and taking into account the need to create synergies between cybersecurity and other parts of Horizon Europe and the Digital Europe Programme: [...] (ii) supporting the cybersecurity industry, in particular SMEs, with a view to strengthening Union excellence, capacity and competitiveness with regard to cybersecurity, including with a view to connecting to potential markets and deployment opportunities, and to attracting investment; and (iii) providing support and technical assistance to cybersecurity start-ups, SMEs, microenterprises, associations, individual experts and civic technology projects;"

The Regulation for implementing a European Competence Centre to monitor and increase the security of network and information systems is less specific on the role supply chains will play. It is mentioned that a cyber-safe design in the whole lifecycle of a system with all the involved organisations and third-parties is necessary to enhance resilience. On the other hand, SMEs represent an essential point of consideration being presented as beneficiaries and thus among the essential stakeholders. This should allow SMEs to receive prepared information and thus also support cybersecurity. This support is intended to ensure that not only resource-rich corporations can position themselves well in cybersecurity but also small SMEs, which can then prepare themselves accordingly for the risk of cyber incidents.

3.4.2.7 *Directive (EU) 2015/2366 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (PSD2)*

The PSD2 is an EU Directive on the regulation of payment services and payment service providers, and the aims are to increase security in payment transactions, strengthen consumer protection, promote innovation and increase competition in the market. This is achieved through two-factor authentication for online payments, secure interfaces for third-party providers and a surcharge ban. This EU Directive was signed and published in 2021 and is currently being reviewed pending an update.

PSD2 partly addresses supply chain and is highlighted in the following box:

Third parties are part of most payment systems; therefore, it must be ensured that third parties are only integrated where necessary to maintain effective competition.

"The provisions relating to access to payment systems should not apply to systems set up and operated by a single payment service provider. Such payment systems can operate either in direct competition to payment systems, or, more typically, in a market niche not adequately covered by payment systems. Such systems include three-party schemes, such as three-party card schemes, to the extent that they never operate as de facto four-party card schemes, for example by relying upon licensees, agents or co-brand partners. Such systems also typically include payment services offered by telecommunication providers where the scheme operator is the payment service provider both to the payer and to the payee, as well as internal systems of banking groups. In order to stimulate the competition that can be provided by such closed payment systems to established mainstream payment systems, it would not be appropriate to grant third parties access to those closed proprietary payment systems. However, such closed systems should always be subject to Union and national competition rules which may require that access be granted to the schemes in order to maintain effective competition in payments markets."

If the performance of the operational functions is dependent on third parties, specific steps must be taken to act in conformity with the underlying Directive.

"Member States shall ensure that, where payment institutions rely on third parties for the performance of operational functions, those payment institutions take reasonable steps to ensure that the requirements of this Directive are complied with."

PSD2 brings significant advantages, especially for the financial flow within supply chains. More payment options can be offered through the integration of international payment companies via secure interfaces. This inevitably leads to a change in the financial supply chain, as the focus is on transactions and liquidity management, as well as customer service. SMEs are not directly related to the PSD2 Directive, as they benefit from it just as much as large companies. However, if SMEs are positioned in the financial sector, PSD2 offers them an excellent opportunity to establish themselves in the financial supply chains, as the barriers to entry have fallen, especially in open banking-powered systems.

3.4.2.8 *Guideline on a Trans-European Automated Real-time Gross settlement Express Transfer system (TARGET2)*

The Eurosystem owns and operates the TARGET2 payment system. It is the main European platform for the settlement of large-value payments and is used by both central banks and commercial banks to settle euro payments in real-time. Modern economies rely on the efficient and secure flow of transactions. Payment systems are the channels through which money can circulate in the economy. TARGET2 is a payment system that allows banks in the EU to send and receive funds in real-time. TARGET2 is used for monetary policy transactions, interbank payments as well as commercial payments by central and commercial banks. TARGET2 provides features that facilitate effective liquidity management, such as payment priority, scheduled transactions, liquidity reserve facilities, limitations, liquidity pooling and optimisation techniques. TARGET2 was introduced on 19 November 2007, and completely superseded

the original TARGET by May 2008. Only supply chain aspects were found in the guidelines of the European Central Bank on Target2-Securities, which are highlighted in the following box:

The participants remain solely liable if third parties are involved in the IT infrastructure.

"Install, manage, operate and monitor and ensure the security of the necessary IT infrastructure to connect to TARGET2-[insert CB/country reference] and submit payment orders to it. In doing so, applicant participants may involve third parties, but retain sole liability. In particular, applicant participants shall enter into an agreement with the network service provider to obtain the necessary connection and admissions, in accordance with the technical specifications in Appendix I;"

Participants also must report security-related incidents in the third-party providers' technical infrastructure.

"Participants shall inform the [insert name of CB] of any security-related incidents in their technical infrastructure and, where appropriate, security-related incidents that occur in the technical infrastructure of the third party providers. The [insert name of CB] may request further information about the incident and, if necessary, request that the participant take appropriate measures to prevent a recurrence of such an event."

If participants provide confidential information to third parties, participants must contract confidentiality requirements with third parties.

"Information relating to the operation of TARGET2-[insert CB/country reference] to which participants have had access, may only be used for the purposes laid down in these Conditions. Participants shall keep such information confidential, unless the [insert name of CB] has explicitly given its written consent to disclose. Participants shall ensure that any third parties to whom they outsource, delegate or subcontract tasks which have or may have an impact on the performance of their obligations under these Conditions are bound by the confidentiality requirements in this Article."

The information and knowledge transfer, pledge or assign by participants to any third party requires written consent by CBs.

"Any rights, interests, obligations, responsibilities and claims arising from or relating to these Conditions shall not be transferred, pledged or assigned by participants to any third party without the [insert name of CB] 's written consent."

TARGET2 has only minor aspects that consider the supply chain. It mainly focusses on reporting security-related incidents if the incident occurs at a third party. Furthermore, the applicants stay liable in case of third-party involvement in the IT infrastructure. The main approaches to ensure that liabilities are confidential agreements and contracts. TARGET2 does not specifically address SMEs.

3.4.2.9 Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS)

The eIDAS Regulation was a significant step towards establishing a predictable regulatory framework. eIDAS facilitates safe and smooth electronic interactions between enterprises, people and public bodies. It ensured that individuals and organisations could use their own national electronic identification systems (eIDs) to access online public services in other Member States. Additionally, it created a unified

European market for trust services by guaranteeing that they function across borders and have the same legal standing as their paper-based counterparts. With eIDAS, the EU has established the proper foundations and a clear legal framework enabling individuals, companies and government agencies to securely access online services and execute transactions with a single click. The implementation of eIDAS provides increased security and convenience for all online operations, such as filing tax returns, enrolling in a foreign university, creating a remote bank account, establishing a company in another Member State, authenticating online payments and submitting online bids.

eIDAS has only minor parts that address supply chain and SME and are highlighted in the following boxes:

If the signatory entrusts qualified electronic signature creation devices to the care of a third-party appropriate mechanisms and procedures must be implemented to ensure appropriate use.

"It should be possible for the signatory to entrust qualified electronic signature creation devices to the care of a third party, provided that appropriate mechanisms and procedures are implemented to ensure that the signatory has sole control over the use of his electronic signature creation data, and the qualified electronic signature requirements are met by the use of the device."

To increase the trust of SMEs in the internal market, eIDAS emphasizes the need to introduce qualified trust services and qualified trust service providers and define requirements and obligations to them.

"To enhance in particular the trust of small and medium-sized enterprises (SMEs) and consumers in the internal market and to promote the use of trust services and products, the notions of qualified trust services and qualified trust service provider should be introduced with a view to indicating requirements and obligations that ensure high-level security of whatever qualified trust services and products are used or provided."

eIDAS has only minor aspects that consider the supply chain. It mainly focusses on third parties outsourcing qualified electronic signature creation devices to the care of a third party. Appropriate mechanisms and procedures must be implemented to ensure control over the use of their electronic signature creation data. Furthermore, eIDAS emphasises the need to increase SME trust by considering their specific needs by introducing qualified trust services and qualified trust service providers and defining requirements and obligations to them.

3.4.2.10 *Directive 2014/53/EU on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (RED)*

RED creates a regulatory framework for the market introduction of radio equipment. It provides a single market for radio equipment by establishing rules for safety and health, electromagnetic compatibility, and effective utilization of the radio spectrum. It also serves as the foundation for subsequent regulations covering several other issues. These include technological safeguards for privacy, personal data and fraud prevention. In addition, other considerations include interoperability, access to emergency services, and compliance concerning the combination of radio equipment and software.

In 2021 the European Commission introduced a delegated act to RED that sought to ensure that all wireless devices marketed in the EU were safe. This legislation established additional legal criteria for cybersecurity measures that manufacturers must include in the affected items' design and manufacturing. It also secures individuals' privacy and personal data, reduces the danger of financial fraud and strengthens the resilience of our communication networks.

The Radio Equipment Directive has several parts that address supply chain which are highlighted in the following box:

Economic operators are responsible for their supply chain compliance with this Directive.

"Economic operators should be responsible for the compliance of radio equipment with this Directive, in relation to their respective roles in the supply chain, so as to ensure a high level of protection of health and safety of persons and of domestic animals, and the protection of property, an adequate level of electromagnetic compatibility, an effective and efficient use of radio spectrum and, where necessary, a high level of protection of other public interests, and to guarantee fair competition on the Union market."

All supply chain members in the radio market equipment must take appropriate measures to ensure the conformity of radio equipment with this Directive.

"All economic operators intervening in the supply and distribution chain should take appropriate measures to ensure that they only make available on the market radio equipment which is in conformity with this Directive. It is necessary to provide for a clear and proportionate distribution of obligations which correspond to the role of each economic operator in the supply and distribution chain."

Traceability throughout the supply chain end-to-end is essential for ensuring radio equipment's conformity with this Directive.

"Ensuring traceability of radio equipment throughout the whole supply chain helps to make market surveillance simpler and more efficient. An efficient traceability system facilitates market surveillance authorities' task of tracing economic operators who made non-compliant radio equipment available on the market. When keeping the information required under this Directive for the identification of other economic operators, economic operators should not be required to update such information in respect of other economic operators who have either supplied them with radio equipment or to whom they have supplied radio equipment."

Threat intelligence and immediate information sharing among Commission and Member States about risks and related supply chain information are essential for this Directive.

"The Member State shall immediately inform the Commission and the other Member States. That information shall include all available details, in particular the data necessary for the identification of the radio equipment concerned, the origin and the supply chain of radio equipment, the nature of the risk involved and the nature and duration of the national measures taken."

While this Directive does not address SMEs specifically, it has far-reaching implications for supply chains. First, it explicitly addresses the supply chain and its members for ensuring radio equipment conformity with the Directive by requiring appropriate measures. Second, it emphasises the need for traceability throughout the whole supply chain. Third, it emphasises the need for information sharing within the EU to share risk and supply chain-related information.

3.4.2.11 Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR)

GDPR stipulates how organisations and businesses must utilise personal data in an integrity-safe manner. Personal data refers to information that might directly or indirectly identify a live individual. Name, telephone number and address are examples of standard personal data. As they may be used to identify a person, interests, information about prior purchases, health and Internet behaviour are also considered personal data.

Data processing includes the collection, structuring, organisation, use, storage, sharing, disclosure, erasure and destruction of data. Every entity that handles personal data (which includes every firm with workers and customers) must guarantee that the personal data it uses complies with the GDPR's standards.

While the Regulation does not address supply chain, it has several SME aspects which are highlighted in the following box:

The GDPR considers the specific situation of SMEs by defining obligations that may not apply to all SMEs.

"In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. The proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping. In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw from Article 2 of the Annex to Commission Recommendation 2003/361/EC (1)."

Codes of conducts developed within this Directive should consider the specific needs of SMEs.

"Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular, such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons."

"The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises."

Activities that raise awareness and education should also include specific measures for SMEs.

"Awareness-raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as natural persons in particular in the educational context."

The specific measures for SMEs are also relevant for implementing this Regulation.

"In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011. In that context, the Commission should consider specific measures for micro, small and medium-sized enterprises."

The specific needs of SMEs for GDPR-related certification should be considered.

"The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account."

In general, the GDPR does not rely on the size of a firm or organisation but rather on the nature of the operations. Activities that pose a significant danger to the rights and liberties of persons, whether conducted by an SME or a major enterprise, prompt the implementation of more restrictive regulations. Nonetheless, certain GDPR rules may not apply to all SMEs.

For example, businesses with less than 250 employees are not required to retain records of their processing operations unless the retention of personal data is a frequent occurrence, constitutes a danger to the rights and freedoms of persons or involves sensitive data or criminal records.

Similarly, SMEs will only be required to appoint a data protection officer if the processing is their primary business and it poses specific threats to the rights and freedoms of individuals (such as the monitoring of individuals or the processing of sensitive data or criminal records), due to the scale of the processing.

3.4.2.12 *Proposal for a regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications – ePrivacy)*

The ePrivacy Regulation (ePR) is a proposal for regulating various privacy-related concerns, mostly on electronic communications inside the EU and will replace the 2002 Privacy and Electronic Communications Directive (ePrivacy Directive) with the GDPR. It will elaborate and supplement the latter concerning privacy-related issues. The secrecy of communications, privacy controls via electronic consent, web browsers and cookies are central to the proposed rule.

This proposal has only minor parts that address supply chain and SMEs which are highlighted in the following boxes:

The record or storage of data related to electronic communications by end-user by third parties must comply with this Regulation.

"After electronic communications content has been sent by the end-user and received by the intended end-user or end-users, it may be recorded or stored by the end-user, end-users or by a third party entrusted by them to record or store such data. Any processing of such data must comply with Regulation (EU) 2016/679."

End-user choices should be binding on and enforceable against any third parties.

"The choices made by end-users when establishing its general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties."

This proposal encourages Member States and their supervisory authorities to consider the SME needs in applying this Regulation.

"Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks set forth in this Regulation. In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have the same tasks and effective powers in each Member State, without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation."

This proposal only has minor aspects related to supply chain and SMEs. It addresses third parties for recording and storing data and allows end-users to enforce their right to third parties. Additionally, this proposal again emphasises the need to consider SME needs in applying the Regulation.

3.4.2.13 *Proposal for a regulation on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 (DORA)*

The EU boosts the IT security of financial institutions such as banks, insurance companies and investment businesses in response to the growing threat of cyber-attacks. In May 2022, the Council President and the European Parliament struck a preliminary agreement on the Digital Operational Resilience Act (DORA), ensuring that the European financial industry can sustain robust operations during a significant operational interruption.

DORA establishes uniform requirements for the security of network and information systems of companies and organisations in the financial sector, as well as critical third parties that provide them with ICT-related services, such as cloud platforms and data analytics services. DORA establishes a legal framework for digital operational resilience, mandating that all businesses ensure their ability to endure, react to and recover from any ICT-related interruptions and threats. These criteria are uniform across all EU Member States. The primary objective is to prevent and neutralise cyber-attacks.

According to the tentative agreement, the new standards will comprise a robust framework enhancing the banking sector's IT security. Therefore, the required efforts of financial institutions will be commensurate with the dangers they face.

Many financial institutions will be subject to the new regulations. Under the terms of the preliminary agreement, auditors will not be subject to DORA, but they will be included in a future assessment of the Regulation, during which time a potential adjustment of the requirements will be considered. In addition, critical third-country ICT service providers to EU financial institutions will be obliged to establish a subsidiary inside the EU for adequate supervision to be implemented.

This proposal has many parts that address supply chain and SME aspects; therefore, only a few highlighted examples are presented in the following boxes:

DORA requires supply chain monitoring and supervision where ICT services support critical functions.

"Where the contractual arrangements on the use of ICT services supporting critical or important functions provide for subcontracting, financial entities shall assess whether and how potentially long or complex chains of subcontracting may impact their ability to fully monitor the contracted functions and the ability of the competent authority to effectively supervise the financial entity in that respect."

DORA emphasises the need for EU harmonisation for digital operational resilience testing and ICT third-party risk monitoring.

"Legislative disparities and uneven national regulatory or supervisory approaches on ICT risk trigger obstacles to the single market in financial services, impeding the smooth exercise of the freedom of establishment and the provision of services for financial entities with cross-border presence. Competition between the same type of financial entities operating in different Member States may equally be distorted. Notably for areas where Union harmonisation has been very limited - such as the digital operational resilience testing - or absent - such as the monitoring of ICT third-party risk - disparities stemming from envisaged developments at national level could generate further obstacles to the functioning of the single market to the detriment of market participants and financial stability."

"This Regulation should thus fill in the gaps or remedy inconsistencies in some of those legal acts, including in relation to the terminology used therein, and should explicitly refer to ICT risk via targeted rules on ICT risk management capabilities, incident reporting, operational resilience testing and third party risk monitoring."

"A certain lack of homogeneity and convergence regarding the monitoring of ICT third party risk and ICT third-party dependencies can be noticed today. Despite efforts to address outsourcing, such as the 2017 recommendations on outsourcing to cloud service providers, the broader issue of counteracting systemic risk which may be triggered by the financial sector's exposure to a limited number of critical ICT third-party service providers is barely addressed by Union legislation. The lack of rules at Union level is compounded by the absence of national rules on mandates and tools that allow financial supervisors to acquire a good understanding of ICT third-party dependencies and to adequately monitor risks arising from concentration of ICT third-party dependencies."

DORA adds to NIS2 and is applicable to all critical third-party service providers.

"The Oversight Framework established by this Regulation applies to all critical ICT third-party service providers, including cloud computing service providers, when they provide ICT services to financial entities and should be considered complementary to the supervision under Directive (add reference to NIS2)."

ICT risk should be addressed holistically by using comprehensive capabilities, policies, and mechanisms for controlling and using processes that address ICT-related incidents and reporting.

"To remain in full control of ICT risk, financial entities need to have in place comprehensive capabilities enabling a strong and effective ICT risk management, alongside specific mechanisms and policies for handling all ICT-related incidents and reporting major ones. Likewise, financial entities should have policies for the testing of ICT systems, controls and processes, as well as for managing ICT third-party risk."

The requirements defined by DORA require the modification of contracts to allow firms to monitor and audit their supply chain partner where necessary.

"This extensive use of ICT services is evidenced by complex contractual arrangements, whereby financial entities often encounter difficulties in negotiating contractual terms that are tailored to the prudential standards or other regulatory requirements they are subject to, or otherwise in enforcing specific rights, such as access or audit rights, when the latter are enshrined in the agreements. Moreover, many such contracts do not provide for sufficient safeguards allowing for a fully-fledged monitoring of subcontracting processes, thus depriving the financial entity of its ability to assess these associated risks. In addition, as ICT third-party service providers often provide standardised services to different types of clients, such contracts may not always adequately cater for the individual or specific needs of the financial industry actors."

Additionally, key principles should guide financial firms in ensuring the fit of their contractual arrangements, as the contractual dimension is not fully anchored in the EU legislation. Additionally, financial firms need guidelines for ICT third-party monitoring.

"Even though the Union financial services legislation contains certain general rules on outsourcing, the monitoring of the contractual dimension is not fully anchored into Union"

legislation. In the absence of clear and bespoke Union standards applying to the contractual arrangements concluded with ICT third-party service providers, the external source of ICT risk is not comprehensively addressed. Consequently, it is necessary to set out certain key principles to guide financial entities' management of ICT third-party risk, which are of a particular importance when financial entities resort to ICT third-party service providers to support their critical or important functions. These principles should be accompanied by a set of core contractual rights in relation to several elements in the performance and termination of contracts with a view to enshrine certain minimum safeguards underpinning financial entities' ability to effectively monitor all risk emerging at ICT third party level. These principles are complementary to sectorial legislation applicable to outsourcing."

"To ensure a sound monitoring of ICT third-party risk in the financial sector, it is necessary to lay down a set of principle-based rules to guide financial entities when monitoring risk arising in the context of functions outsourced to ICT third-party service providers, particularly for ICT services supporting the critical or important functions, as well as more generally in context of all ICT third-party dependencies."

DORA emphasises the need to consider the specific needs of SMEs and the structure of the insurance intermediation market.

"In addition this Regulation acknowledges the specificities of the insurance intermediation market structure, with the result that insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries qualifying as microenterprises, small or medium-sized enterprises should not be subject to this Regulation."

"Under sector specific Union legislation some financial entities are subject to lighter requirements or exemptions for reasons associated with their size or the services they provide. These categories include small and non-interconnected investment firms, small institutions for occupational retirement provision which may be excluded from the scope of Directive (EU) 2016/2341 under the conditions laid down in Article 5 of that Directive by the Member State concerned and operate pension schemes which together do not have more than 100 members in total as well as institutions exempted under Directive 2013/36/EU."

"This Regulation shall not apply to ... insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries which are microenterprises, small or medium-sized enterprises."

Article 14a of the proposal specifies a simplified ICT risk management framework that is applicable to SMEs.

"Articles 4 to 14 of this Regulation shall not apply to small and non-interconnected investment firms, payment institutions exempted pursuant to Directive (EU) 2015/2366; institutions exempted pursuant to Directive 2013/36/EU in respect of which Member States have decided not to apply the option referred to in Article 2(4), electronic money institutions exempted pursuant to Directive 2009/110/EC; and small institutions for occupational retirement provision."

With DORA, the EU urges the European financial industry to handle ICT and third-party risks with more control and efficiency. It is anticipated that an oversight structure encompassing the whole supply chain will be in place regarding security measures. This includes ICT third-party providers, ICT-related service providers, and communications technology ICT risk to cloud service providers and ICT-related events.

The purpose of the DORA is to guarantee that companies have the procedures, tools, and people required to continuously detect and mitigate third-party risk. Additionally, DORA requires financial institutions to include ICT third-party risk management criteria in contracts with third-party service providers. These criteria focus on three main areas:

1. Companies must have a well-defined policy and plan for third-party risk. The regulator expects clear buy-in from management, which is conveyed across the company as an executable strategy.
2. EU financial companies must do their due diligence before any commercial engagement. It is essential to comprehend the degree of danger a third party poses. Consequently, it is essential to comprehend the security posture of third-party or subcontracting concerns.
3. Businesses must clearly understand how ICT contractual service needs translate to the financial/business services offered by their suppliers. Understanding the importance of the financial/business service permits business continuity planning. In addition, the execution of risk management criteria has a greater likelihood of success when the possible effect is estimated.

DORA focuses primarily on ICT third-party service providers. The advice to financial institutions seems to be "trust but verify your third-party service providers." In terms of assurance, this implies that enterprises may legally require proof of a provider's security posture. This proposal is an excellent tool for information security experts to obtain assurance from ICT third parties, such as penetration testing reports, vulnerability scans, source code inspections and third-party risk surveys. The objective is to guarantee that providers implement testing standards across their company. More significantly, they have a sound security posture and mitigate discoveries.

Additionally, it is recommended that financial institutions enhance their management and surveillance of third-party ICT suppliers. This is done to lessen the possible threats associated with their significant dependencies. Financial institutions are being encouraged by regulators to take more responsibility and assess the operational resilience of their key third-party dependent services. In a worst-case scenario, the financial stability of European markets might be at risk.













3.4.3 Recommendation/gaps















The analysis shows that the EU fosters security by considering aspects that are related to supply chains and SMEs via several means. The identified regulations address different but similar fields, from supply chain liability to monitoring and traceability. More than ten regulations could be identified, often aiming at the same aspects concerning supply chains and SMEs. A possible explanation is that even though the necessary regulatory framework at the European level is in place, most regulations focus on specific parts of the economy, such as finance-oriented regulations. Consequently, the aspects considering supply chain and SME are realised very differently, as the table below indicates.

Furthermore, the analysis also showed that most regulations only have one aspect involved relating to supply chains or SMEs. Only the recently published proposals for NIS2, Due Diligence and DORA address both aspects fully. As attackers also increasingly focus on supply chain vulnerabilities, the recently published proposals reflect the dynamic environmental development. They also emphasise the requirement for addressing SME-specific needs which should consider the lack of cybersecurity

awareness in many SMEs. From a supply chain view, we must emphasise that RED has one of the most far-reaching implications for supply chains as it requires supply chain traceability.

The results of the analysis are shown in a traffic light system in the following table to visualise the results of the legal analysis and to depict the degree of consideration of supply chain and SME aspects in the reviewed regulations. The colour red indicates that the single regulation does not address aspects of supply chain or SME. Yellow indicates that supply chain or SME aspects are addressed partly by the single regulation. Green indicates that the single regulation addresses supply chain or SME aspects. Finally, the table also presents examples that are supply chain and SME-related.

Regulation	Aspects		Examples	
	Supply chain	SME	Supply chain	SME
NIS1			Reporting of dependencies	Information sharing with SMEs.
NIS2			Consideration of the whole product development cycle, supply chain risk assessments.	SME-specific criteria for SMEs, further guidance through policies.
Cyber Resilience Act			Supply chain-wide vulnerability analysis, continuous risk assessment process.	SME-friendly fees.
Cybersecurity Act			Important lens for cybersecurity.	Important stakeholder in the development.
Due Diligence			Supply chain traceability, supply chain, and risk-related information sharing, continuous supply chain risk management assessments.	Reduced scope of guidelines for SMEs, providing support for SMEs.
ECCC			Update regulation for third parties after the end-of-service of products.	Important stakeholder, SME-specific assistance.

PSD2			Update regulation for third parties after the end-of-service of products.	N/A
Target2			Incident reporting, liability for third parties.	N/A
EIDAS			Outsourcing, appropriate measures, and procedures for ensuring control of third parties.	Define trust services to increase SME trust.
RED			Supply chain conformity, supply chain traceability, supply chain and risk-related information sharing.	N/A
GDPR			N/A	Certain rules do not apply to all SMEs.
ePrivacy			Rules for third parties	Consideration of SME needs.
DORA			Supply chain monitoring and supervision address ICT-related risks in supply chains holistically.	Consideration of SME needs.

The recommendations based on the regulatory analysis include the following:

- Recommendation 1:** It is recommended to continue including supply chain and SME aspects in future proposals and regulations and defining specific aspects of how supply chain and SME operate should be considered. Cybersecurity in the EU requires increased regulatory considerations of supply chains and we recommend continuing to increase those requirements; for example, traceability for cybersecurity is not only relevant for radio equipment and could (and should) be applied elsewhere. The supply chain focus allows a broad economic impact compared to single-firm set of considerations: for example, NIS2, Due Diligence and DORA are already a step in the right direction for ensuring supply chain cybersecurity in the EU..
- Recommendation 2:** It is recommended to harmonise further the supply chain and SME dimensions considered in the analysed current and future regulations and for seeking clarification

whenever possible. The analysis shows that the supply chain and SME-related perspectives addressed vary a lot between the different regulations and directives. Needless to say, this approach of looking across the board at European legislation through the lens of one of more topic would be highly beneficial in reducing confusion and maximising impact in many areas.

4 Summary and next steps

4.1 A summary of threats / risks, opportunities and recommendations

The report leveraged the work carried out in deliverable D9.12, particularly in the area of recommendations, most of which were considered to be still valid aspirations. The report formed a narrative of contributions from other work carried out in CyberSec4Europe and beyond. The groundwork was laid in a summary of the technological and market analysis from the supply chain roadmapping activity (in WP4). This resulted in a summation of the technological opportunities seen for supply chain security, which was followed by a deep dive into an evaluation of the results derived from the supply chain demonstrator use cases and the use of blockchain as a means of providing secure, reliable and trustworthy transactions in supply chains.

In addition, we looked at the training and education actions required to support a greater awareness of cybersecurity in supply chain scenarios (from WP9) not just for SMEs but all the actors involved in order that the technology recommendations can be implemented.

Finally, we carried out an analysis of thirteen regulations and directives, those both in force and proposed, looking at each from the dual perspectives of supply chain and SMEs which resulted in the conclusion that a greater deal of harmonisation could / should take place among regulators.

4.2 Recommended next steps for EU funding and/or regulation

This report contains three sets of recommendations in addition to the ones identified in the previous report in this series which are summarised in [section 3.2](#).

4.2.1 Regulatory

- It is recommended to continue including supply chain and SME aspects in future proposals and regulations and defining specific aspects of how supply chain and SME operate should be considered. Cybersecurity in the EU requires increased regulatory considerations of supply chains and we recommend continuing to increase those requirements; for example, traceability for cybersecurity is not only relevant for radio equipment and could (and should) be applied elsewhere. The supply chain focus allows a broad economic impact compared to single-firm set of considerations: for example, NIS2, Due Diligence and DORA are already a step in the right direction for ensuring supply chain cybersecurity in the EU.
- It is recommended to harmonise further the supply chain and SME dimensions considered in the analysed current and future regulations and for seeking clarification whenever possible. The analysis shows that the supply chain and SME-related perspectives addressed vary a lot between the different regulations and directives. Needless to say, this approach of looking across the board at European legislation through the lens of one of more topic would be highly beneficial in reducing confusion and maximising impact in many areas.

4.2.2 EU funding

The provided implementations and their validation demonstrate the technical feasibility of realising complex, highly distributed supply chains in a secure manner. We can conclude that blockchain-based architectures represent an appropriate technology to implement supply chain scenarios that cannot rely on a trusted third party i.e., where it is not possible to agree on and operate a trusted third party but where partners demand to have (shared) control of the infrastructure and data. We provided an example that demonstrated how an infrastructure was realised in a way spans different regions and organisations.

Nevertheless, we pointed out that the realisation and operation of blockchain-based architectures is not without additional costs compared to centrally operated systems. This refers to higher efforts due to the complexity of the overall distributed system architecture itself and regarding operational efforts, e.g., for hosting peers, orderers and clients of the Hyperledger Fabric network. Supply chain partners must be able and willing to take over these additional responsibilities and must decide between the trade-off of costs for infrastructure and operation versus autonomy or independence from a trusted third party.

For SMEs, this may be a barrier that prevents them from participating at this time. To tackle this dilemma, good tool support for the definition and roll-out of blockchain-based infrastructures is needed. Therefore, we encourage future research and development to focus on technologies and tools for easing the definition, roll-out and verification of secure and reliable distributed architectures. The to-be developed technologies should, ideally, support the high-level process from workflow specification via automated creation and roll-out up to its verification. The goal would be that the (semi-) automated creation of the deployment configuration (including smart contracts, channel configuration, and private data collections) can be done based on the specification of the workflow. This would significantly contribute to reducing the overall complexity of the creation process. Additionally, tool support for the distributed deployment is needed to ease the setup of required channels, deploying the contracts and other components. Finally, tool support for the validation of correct instantiations is needed. In particular, the created blockchain network configuration must be validated with respect to the workflow specification requirements. This process is currently manual work and should be further automated with (open-source) tooling.

To sum up, based on the experience gained through our evaluation of prototypes, our recommendations are:

- (1) continuing research and development in blockchain and workflow technologies for their integration in distributed supply chain systems and to address the identified gaps.
- (2) increasing the maturity of tools and blockchain technologies (e.g., as part of open-source developments) to improve the usability of the deployed systems and thus increase industry adoption, especially among SMEs.

4.2.3 *Training and education*

We highlighted a set of recommendations and best practices from a wide range of organisations, in both the public and private spheres. It was clear that supply chain incorporates all three pillars of cybersecurity: people, process and technology. Unfortunately, human employees often do not have a good reputation in organisational cybersecurity. In 2022, around 82% of data breaches contained human elements, including social attacks, errors and misuse [Verizon2022]. This is why NIST's C-SCRM guidelines place a heavy emphasis on cybersecurity awareness and training for individuals throughout the supply chain. Many national agencies, projects and private organisations, some of which we listed, offer awareness and training on cyber supply chains.

5 References

- [Adams05] C. Adams. “Impersonation Attack”, in H. C. A. van Tilborg (ed.) Encyclopedia of Cryptography and Security, Boston, MA, https://doi.org/10.1007/0-387-23483-7_196, Springer, 2005.
- [Alickaj18] D. Alickaj and P. Bowhay, “Opus & Ponemon Institute Announce Results of 2018 Third-Party Data Risk Study: 59% of Companies Experienced a Third-Party Data Breach, Yet Only 16% Say They Effectively Mitigate Third-Party Risks”, Businesswire, San Francisco, CA, USA, 15 November 2018.
- [Alicke2020] K. Alicke, R. Gupta, and V. Trautwein, “Resetting supply chains for the next normal”, McKinsey & Company, July 2021, <https://www.mckinsey.com/capabilities/operations/our-insights/resetting-supply-chains-for-the-next-normal>
- [Androulaki2018] E. Androulaki, S. Cocco und C. Ferris, „Private and confidential transactions with Hyperledger Fabric,“ IBM, 11 May 2018. [Online]. Available: <https://developer.ibm.com/technologies/blockchain/tutorials/cl-blockchain-private-confidential-transactions-hyperledger-fabric-zero-knowledge-proof/>
- [Ashraf2022] M. Ashraf, “The war in Ukraine: A moment of reckoning for the oil and gas industry”, Accenture, May 2022, <https://www.accenture.com/us-en/insights/energy/ukraine-oil-gas>
- [Bieliauskaite2018] J. Bieliauskaite, "New SME Guide on Information Security Management: the standard ISO27001 made easy for SMEs," European Digital SME Alliance, <https://www.digitalsme.eu/new-sbs-guide-information-security-management-standard-iso27001-made-easy-smes/>. 2018
- [Boyens2022] J. Boyens, A. Smith, N. Bartol, K. Winkler, A. Holbrook and M. Fallon, “Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations,” NIST, Gaithersburg, MD, USA, May 2022.
- [BSI2022] BSI, “Supply Chain Services and Solutions,” [Online]. Available: <https://www.bsigroup.com/en-US/our-services/supply-chain-solutions/solutions-services/training/>. [Accessed 11 November 2022].
- [CCSB2020] Center for Cyber Security Belgium, “Supply Chain Process 2020 Guidelines,” Center for Cyber Security & Chancellery of the Prime Minister, Brussels, Belgium, 2020.
- [CISA2022] CISA, “Cyber Supply Chain Risk Management,” [Online]. Available: <https://niccs.cisa.gov/education-training/catalog/federal-virtual-training-environment-fedvte/cyber-supply-chain-risk>. [Accessed 9 November 2022].
- [CS4ED45] E. Markatos et al. “D4.5 Research and development roadmap 3”, CyberSec4Europe, https://cybersec4europe.eu/wp-content/uploads/2022/02/D4.5-Research-and-Development-Roadmap-3_v6_submitted.pdf. January 2022.
- [CS4ED51] CyberSec4Europe, D5.1: Requirements Analysis of Demonstration Cases Phase 1, <https://cybersec4europe.eu/wp-content/uploads/2020/06/D5.1-Requirements-Analysis-of-Demonstration-Cases-Phase-1-v3.0.pdf>. May 2019
- [CS4ED54] CyberSec4Europe, D5.4: Requirements Analysis of Demonstration Cases Phase 2, <https://cybersec4europe.eu/wp-content/uploads/2021/05/D5.4-Requirements-Analysis-of-Demonstration-Cases-Phase-2-v1.0-submitted.pdf>. May 2021

- [CS4ED55] CyberSec4Europe, D5.5: Specification and set-up demonstration case Phase 2, https://cybersec4europe.eu/wp-content/uploads/2022/01/D5.5-Specification-and-set-up-demonstration-case-Phase-2-v1.0_submitted.pdf. December 2021
- [CS4ED56] CyberSec4Europe, D5.6: Validation of Demonstration Case Phase 2, <https://cybersec4europe.eu/wp-content/uploads/2022/12/D5.6-Validation-Demonstration-Case-Phase-2-Final-submitted.pdf>. November 2022
- [CyberMAR2022], “Cyber-MAR: Cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain,” [Online]. Available: <https://www.cyber-mar.eu/>. [Accessed 15 November 2022].
- [Cyberwatching2022] Cyberwatching.eu, “Cybersecurity and Privacy Marketplace,” [Online]. Available: <https://www.cyberwatching.eu/market-products-list>. [Accessed 16 November 2022].
- [EC] European Commission, “Standardisation and SMEs”, https://ec.europa.eu/growth/smes/sme-strategy/access-to-markets/standardisation_en#:~:text=Standardisation%20brings%20many%20benefits%20to,capacity%2C%20and%20enhance%20their%20competitiveness.
- [EDPS22] EDPS, “The future of data protection: effective enforcement in the digital world”. <https://www.edpsconference2022.eu/>
- [ENISA2014] ENISA. “Secure ICT Procurement in Electronic Communications.” December 2014. Accessed November 2021. <https://www.enisa.europa.eu/publications/secure-ict-procurement-in-electronic-communications/>
- [ENISA2015] ENISA. “Supply Chain Integrity: An overview of the ICT supply chain risks and challenges, and vision for the way forward.” September 2015. Accessed November, 2021. <https://www.enisa.europa.eu/publications/sci-2015>
- [ENISA2019a] ENISA. “Industry 4.0 Cybersecurity: Challenges & Recommendations.” May 2019. Accessed November, 2021. <https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations>
- [ENISA21] ENISA, “Threat Landscape for Supply Chain Attacks,” <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>, July 2021.
- [ENISA22a] ENISA. “ENISA Threat Landscape for Ransomware Attacks”, July 2022.
- [ENISA22b] ENISA. “ENISA Threat Landscape 2022”, October 2022.
- [EUCS20] European Commission. “Joint Communication: The EU’s Cybersecurity Strategy for the Digital Decade”. December 2020.
- [EUGD2019] European Green Deal, 2019, <https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal>
- [Forescout22] Forescout. “Analysis of Conti Leaks”, March 2022.
- [GDPR19] GDPR.EU, “GDPR small business survey: Insight from European small business leaders one year into the General Data Protection Regulation”. <https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf>

- [GDPR21a] J. Henderson, D. Mack and M. Tichon, “Ready for Supply Chain’s General Data Protection Regulations?”, May 2021, https://www.supplychain247.com/article/ready_for_supply_chains_general_data_protection_regulation
- [GLSystems2022] G. L. Systems, “Supply Chain Cyber Attacks: A 2022 Cybersecurity Outlook,” [Online]. Available: <https://globallearningsystems.com/supply-chain-cyber-security/>. [Accessed 15 November 2022].
- [Goodman2022] D. Goodman, A. Pasic, E. Suni, J. Paijanen, G. Erdogan, K. Bernsmed, P. Meland and S. Tokas, “D9.19 Exploitation Strategy Report 2,” CyberSec4Europe, https://cybersec4europe.eu/wp-content/uploads/2022/02/D9.19-Exploitation-Strategies-Report-4.0_submitted.pdf, 2022.
- [Hoffmann2022] B. Hofmann, P. Kasinathan, M. Wimmer, Towards achieving confidentiality in Hyperledger Fabric, <https://ieeexplore.ieee.org/document/9881834>, August 2022
- [ISO] ISO, "ISO and Small and Medium Enterprises", <https://www.iso.org/iso-and-smes.html#:~:text=ISO%20International%20Standards%20help%20businesses,requirements%2C%20at%20a%20lower%20cost>.
- [Kasinathan2021] P. Kasinathan, D. Martintoni, B. Hofmann, V. Senni, M Wimmer, Secure Remote Maintenance via Workflow-Driven Security Framework, <https://ieeexplore.ieee.org/author/37085422527>, December 2021
- [Lemay18] A. Lemay, J. Calvet, F. Menet, J. M. Fernandez. “Survey of publicly available reports on advanced persistent threat actors”, Computers & Security 72, pp. 26-59, 2018.
- [Matt22] M. Burgess. “How GDPR Is Failing”. Wired, May 2022.
- [McCann22] McCann FitzGerald. “General Data Protection Regulation: A survey of the impact of GDPR and its effect on organisations in Ireland”. January 2022.
- [McKinsey20] J. Manyika, S. Smit, J. Woetzek. “Risk, resilience, and rebalancing in global value chains”, McKinsey Global Institute, 2020.
- [MS22] Microsoft. “Microsoft Digital Defense Report 2022”, November 2022.
- [NCSC2022] National Cyber Security Centre, “Supply chain security guidance,” [Online]. Available: <https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security>. [Accessed 27 10 2022].
- [NIS2022] Cyber Risk GmbH, “The NIS 2 Directive”, May 2022, <https://www.nis-2-directive.com>
- [NIST2018] NIST, “Cybersecurity Framework”, version 1.1, 2018, <https://www.nist.gov/cyberframework>
- [NIST2022a] NIST, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, SP800-161 Rev.1, May 2022, <https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final>
- [NIST2022b] NIST, “Best Practices in Cyber Supply Chain Risk Management,” [Online]. Available: <https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf>. [Accessed 14 November 2022].
- [NIST21] NIST, “Defending Against Software Supply Chain Attacks,” National Institute of Standards and Technology,

- https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf, April 2021.
- [Nozomi22] Nozomi Networks. “OT/IoT Security Report. Cyber War Insights, Threats and Trends, Recommendations”. August 2022.
- [PaloAlto22] Paloalto networks, “Extortion Payments Hit New Records as Ransomware Crisis Intensifies”, August 2021, <https://www.paloaltonetworks.com/blog/2021/08/ransomware-crisis/>
- [Peisert21] S. Peisert, et al. “Perspectives on the SolarWinds incident”, IEEE Security & Privacy 19, no. 2, pp. 7-13, 2021.
- [SANS2022] SANS Institute, “Integrating Software Supply Chain Security into Security Operations,” [Online]. Available: <https://www.sans.org/webcasts/integrating-software-supply-chain-security-into-security-operations/>. [Accessed 15 November 2022].
- [SBS] Small Business Standards, "The Voice of European SMEs in Standardisation", <https://www.sbs-sme.eu/standards/what-standard>.
- [Schäfer 2018] Schäfer, Matthias. "The fourth industrial revolution: How the EU can lead it." *European View* 17, no. 1 (2018): 5-12.
- [SCOR22] SCOR, The Art & Science of Risk, “Cybersecurity of the Supply Chain”, September 2022, <https://www.scor.com>
- [SGD-7] United Nations, “Affordable and Clean Energy” (Goal 7), <https://www.un.org/sustainabledevelopment/energy/>
- [SITA21] SITA statement about security incident. <https://www.sita.aero/pressroom/news-releases/sita-statement-about-security-incident/>. March 2021.
- [Sonatype22] Sonatype. “8th State of the Software Supply Chain”, <https://www.sonatype.com/state-of-the-software-supply-chain/>. October 2022.
- [Souppaya2022] M. Souppaya, K. Scarfone and D. Dodson, “Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities,” National Institute of Standards and Technology, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf>, February 2022
- [USBill21] The White House. “Executive Order 14028, Improving the Nation’s Cybersecurity”, May 2021.
- [Verizon2022] Verizon, “Data Breach Investigations Report,” <https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf>, 2022.