EUROPEAN UNION AGENCY
FOR CYBERSECURITY

GOOD PRACTICES FOR SUPPLY CHAIN CYBERSECURITY

JUNE 2023

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) is the EU's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost the resilience of the EU's infrastructure and, ultimately, to keep Europe's society and people digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors, please use resilience@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu

AUTHORS

Maria Papaphilippou, Konstantinos Moulinos, Marianthi Theocharidou

ACKNOWLEDGEMENTS

Volker Distelrath, Siemens

LEGAL NOTICE

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to Regulation (EU) 2019/881.

ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source.

Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication.

Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2023

Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (https://creativecommons.org/licenses/by/4.0/). This means that reuse is allowed provided appropriate credit is given and any changes are indicated.

For any use or reproduction of photos or other material that are not owned by ENISA, permission may need to be sought directly from the respective right holders.

ISBN 978-92-9204-636-1 doi:10.2824/805268 TP-03-23-145-EN-N

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Directive (EU) 2022/2555 (the NIS2 directive) [1] requires Member States to ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems, which those entities use in the provision of their services. Supply chain cybersecurity is considered an integral part of the cybersecurity risk management measures under Article 21(2) of the NIS2 directive.

The report provides an overview of the current supply chain cybersecurity practices followed by essential and important entities in the EU, based on the results of a 2022 ENISA study which focused on investments of cybersecurity budgets among organisations in the EU.

Among the findings the following points are observed.

- 86 % of the surveyed organisations implement information and communication technology / operational technology (ICT/OT) supply chain cybersecurity policies.
- 47 % allocate budget for ICT/OT supply chain cybersecurity.
- 76 % do not have dedicated roles and responsibilities for ICT/OT supply chain cybersecurity.
- 61 % require security certification from suppliers, 43% use security rating services and 37% demonstrate due diligence or risk assessments. Only 9 % of the surveyed organisations indicate that they do not evaluate their supply chain security risks in any way.
- 52 % have a rigid patching policy, in which only 0 to 20 % of their assets are not covered. On the other hand, 13.5 % have no visibility over the patching of 50 % or more of their information assets.
- 46 % patch critical vulnerabilities within less than 1 month, while another 46 % patch critical vulnerabilities within 6 months or less.

The report also gathers good practices on supply chain cybersecurity derived from European and international standards. It focuses primarily on the supply chains of ICT or OT. Good practices are provided and can be implemented by customers (such as organisations identified as essential and important entities under the NIS2 directive) or their respective suppliers and providers. The good practices cover five areas, namely:

- strategic corporate approach;
- supply chain risk management;
- supplier relationship management;
- vulnerability handling;
- quality of products and practices for suppliers and service providers.

Finally, the report concludes the following.

- There is confusion with respect to terminology around the ICT/OT supply chain.
- Organisations should establish a corporate-wide supply chain management system based on third party risk management (TRM) and covering risk assessment, supplier relationship management, vulnerability management and quality of products.
- Good practices should cover all various entities which play a role in the supply chain of ICT/OT products and services, from production to consumption.
- Not all sectors demonstrate the same capabilities concerning ICT/OT supply chain management.
- The interplay between the NIS2 directive and the proposal for a cyber resilience act or other legislation, sectorial or not, which provides cybersecurity requirements for products and services, should be further examined.

[1] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80). https://eur-lex.europa.eu/eli/dir/2022/2555

1. INTRODUCTION

Surveys from the World Economic Forum (WEF) and Anchore report that between **39 %** [2] **and 62 %** [3] **of organisations were affected by a third-party cyber incident**. Moreover, according to Mandiant [4], **supply chain compromises were the second most prevalent initial infection vector** identified in 2021. They also account for 17 % of the intrusions in 2021 compared to less than 1 % in 2020.

In 2021, ENISA's Threat landscape for supply chain attacks shows that in 66 % of the supply chain attacks analysed, **suppliers did not know, or were not transparent** about, how they were compromised. In contrast, less than 9 % of the customers compromised through supply chain attacks did not know how the attacks happened. This highlights the gap in terms of maturity in cybersecurity incident reporting between suppliers and end-user facing companies. Around 62 % of the attacks on customers took advantage of their **trust in their supplier**. In 62 % of the cases, **malware** was the attack technique employed. When considering targeted assets, in 66 % of the incidents, attackers focused on the **suppliers' code** in order to further compromise targeted customers.

The latest ENISA threat landscape report (2022) also observes an increased interest of threat groups in **supply chain attacks and attacks against** managed service providers (MSPs) [5]. Moreover, the report considers it likely that we will see an increased investment [6] of resources into **vulnerability research** in these supply chains in the near future. This is one of the reasons why threat groups have been targeting security researchers directly. Another target is common and popular **open-source repositories** like NPM, Python, and RubyGems, which are either cloned on infected with malware, with the goal of infecting anyone who implements these as tools or packages within their project. As anyone can publish packages to open-source platforms, malware injection often remains under the radar for a long time.

It is, therefore, evident that cyber risks arising from partners, suppliers and vendors could have systemic implications. This is also confirmed by the results of a recent survey among cyber leaders and CEOs [7] – almost 40 % of respondents said they were negatively affected by a cybersecurity incident relating to their third-party vendors / supply chain. The rise in incidents has concerned the majority of the surveyed CEOs (58 %), who indicated that they feel their partners and suppliers are less resilient than their own organisation. This will result in the greatest influence on their organisations' approach to cybersecurity in the future.

1.1 SUPPLY CHAIN IN THE NIS2 DIRECTIVE

In this complex environment of supply chains, establishing good practices for supply chain cybersecurity at the EU level is now more important than ever. The NIS2 directive[1] enhances supply chain cybersecurity by:

- eliminating the distinction between operators of essential services and digital service providers;
- extending the coverage to a larger portion of the economy and society by adding more sectors with the differentiation of essential and important entities;
- addressing supply chain cybersecurity and supplier relationship by requiring individual entities to address respective cybersecurity risks;
- introducing focused measures including incident response and crisis management, vulnerability handling and disclosure, cybersecurity testing and the effective use of encryption;
- introducing accountability of each entity's management for compliance with cybersecurity risk management measures;
- suggesting that the NIS Cooperation Group may carry out coordinated security risk assessments of specific critical information and communication technology (ICT) services, systems or products.

[2] WEF, Global Cybersecurity Outlook 2022. https://www.weforum.org/reports/global-cybersecurity-outlook-2022/
[3] Anchore, '2022 security trends: Software supply chain survey. https://anchore.com/blog/2022-security-trends-software-supply-chain-survey/
[4] Kutscher, J., 'M-TRENDS 2022', Mandiant. https://www.mandiant.com/resources/m-trends-2022
[5] ENISA Threat Landscape 2022 report.
[6] PWC 2022 Global Digital Trust Insights Survey. https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html
[7] WEF, Global Cybersecurity Outlook 2022. https://www.weforum.org/reports/global-cybersecurity-outlook-2022/

The NIS2 directive requires essential and important entities to address cybersecurity risks in supply chains and supplier relationships. It does so by requesting in Article 21 essential and important entities to take appropriate and proportionate technical, operational and organisational cybersecurity risk management measures and to follow an all-hazards approach. These measures should address, amongst other areas, supply chain security including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers. Moreover, entities should take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.

Member States shall also ensure that, when defining appropriate measures, entities are required to take into account the results of the coordinated risk assessments carried out in accordance with Article 22(1) [8].

1.2 AIM AND AUDIENCE

The aim of this report is to provide an overview of the current ICT / operational technology (ICT/OT) supply chain cybersecurity practices followed by the operators in the EU as well as to identify **good practices on ICT/OT supply chain cybersecurity**. The report focuses primarily on the relationship of **essential and important entities** with different kinds of **direct suppliers and service providers** [9], e.g. manufacturers, distributors, integrators, MSPs, managed security service providers (MSSPs) or cloud computing service providers. It thus identifies good practices for essential and important entities, and for different types of suppliers and providers.

Essential and important entities typically operate critical infrastructure and use products, systems and solutions from manufacturers, distribution channel providers, system integrators and digital service providers. Some entities do manufacture their own products (hardware and software) and can in this case be considered as important entities too. Recommended good practices for manufacturing can be applied for such organisations as well.

An entity typically has a contractual relation with its direct suppliers and service providers where organisational, process and technical measures can be defined for respective delivery or service acquired. The range of contractual agreeable measures is limited to the procurement power of an organisation and the capabilities of a supplier or service provider. Some measures cascade along the supply chain, but the overall control of implementation by a respective organisation is typically not possible, as there is no general contractual relation in place which could for example provide an audit right or the right to request detailed information on security measures from all suppliers along the supply chain. One typical example of this lack of control in the supply chain of products and components is the open-source software, which is publicly available and the rules of use of which are determined in non-negotiable license agreements. Another example of the need to maintain control is when procuring services from a cloud computing service provider, as this requires additional effort to ensure that the requirements of the General Data Protection Regulation are met.

Table 1 includes a brief description of the role of the various types of suppliers and providers in the ICT/OT supply chain.

Table 1: Suppliers and providers

Type of supplier and provider	Function
Manufacturers [10]	• Design, develop, manufacture, and deliver products and components to their customers. • Source hardware and software components in their supply chain. • Deliver products which can serve multiple purposes; i.e. similar products are sold to different product users with different use scenarios. • Liable for their part of delivery and service provided.
System integrators (service providers	• Engineer systems that are used in production environments. • Design and deploy systems, such as automation solutions used in industries and critical infrastructure.

[8] EU coordinated risk assessments of critical supply chains.
[9] NIS2 directive, Article 21(2), point (d).
[10] Important entities (NIS2 directive, Annex II).

for engineering services)	• Can include civil work such as deployment of network infrastructure or pipelines for example in turnkey solutions. • Play an essential part in cybersecurity design and implementation in (critical) infrastructure.
ICT service management	Managed Service Providers (MSPs) • Provide services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers' premises or remotely.

	MSSP
	• Assists entities in areas such as incident response, penetration testing, security audits and consultancy (NIS2 directive, Article 6(40)).
	• Offers services, such as:
	  • assessment – e.g. penetration testing, or conformance to specific security requirements or standards;
	  • implementation – e.g. implementation of security controls such as malware detection in an infrastructure;
	  • management – e.g. security operating centre (SOC) services for incident response.

Providers of digital services [11] [12]	Cloud computing services, include: • infrastructure as a service, • platform as a service, • software as a service (SaaS), and • network as a service.

In this report, supply chain cybersecurity measures will be recommended for providers of digital services that fall into the category of SaaS. Examples of such a service are digital tax-accounting services [13], multi-tenant asset monitoring services [14], security operating centre services [15] or even supply chain services [16].

Addressing supply chain cyber risks requires a risk-based approach from organisations in the supply chain. This report will address cybersecurity risks for the supply chain, but will not touch other supply chain risks, such as geopolitical risks like dependencies on non-EU country shipments, e.g. photovoltaic (PV) inverter or chipset for electronic devices which are nearly entirely sourced in Asia [17].

1.3 METHODOLOGY AND STRUCTURE

In an effort to identify how Member States implemented the NIS directive's requirements, and whether they invest in cybersecurity, ENISA surveyed 1 081 organisations in all 27 Member States (and to ensure a representative account,

[11] A digital service is defined by NIS2 directive, Article 6.
Clause (23): 'digital service' means a service within the meaning of Article 1(1)(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council.
Clause (28): 'online marketplace' means a digital service within the meaning of Article 2 point (n) of Directive 2005/29/EC of the European Parliament and of the Council.
Clause (29): 'online search engine' means a digital service within the meaning of Article 2(5) of Regulation (EU) 2019/1150 of the European Parliament and of the Council.
Clause (30): 'cloud computing service' means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including when those are distributed over several locations.
[12] Essential entities (NIS2 directive, Annex I, 'Digital Infrastructure').
[13] Digital tax-accounting services offering cloud-based solutions for the handling of tax, e.g. the EU mini One Stop Shop for value-added-tax declaration is such an example.
[14] Multi-tenant asset monitoring services offer customers for example a health status service for assets used in their respective infrastructure (e.g. turbines) that can optimise maintenance schedules and replacements.
[15] SOC is a managed security service; the offering is typically realised by a digital cloud service where customers are provided with a dashboard on findings that are derived from analytics on security information delivered from the network by utilising a cloud-based security information event management system. Consequently, a SOC service belongs in the category of a digital service provider as well as in the category of an MSSP.
[16] Digital supply chain as a service offers customers tracking and control options via a cloud-based solution to manage their supply chain. This includes tracking of goods that are en route and the management of goods in warehouses.
[17] China's sanctions against Taiwan are a reminder for the European Union of its dependency on the island, and in particular on the electronic chips produced by the world's biggest semiconductor company: Taiwan Semiconductor Manufacturing Co.

a minimum of 40 organisations were surveyed per Member State) [18]. Among other things, data was collected concerning ICT/OT supply chain cybersecurity. Organisations were requested to provide information relating to their implemented supply chain risk management policies and whether they allocate budget specific to these issues. They were also surveyed regarding their assigned supply chain risk management roles and responsibilities, the implemented risk mitigation methodologies and whether the EU cybersecurity requirements affect digital products.

Chapter 2 presents the results of this survey and provides an overview of the current practices of essential and important entities relating to supply chain cybersecurity. This allows for a better understanding of the current situation in the EU.

For this report, good practices were collected from relevant standards and guidance that would be appropriate for the implementation of the NIS2 directive's requirements by essential and important entities [19]. In order to identify these good practices, an extensive desktop research was performed on existing supply chain national strategies, regulatory frameworks, standards and good practices. As a result, 19 relevant documents that address supply chain cybersecurity were identified and analysed. The analysis reflects on existing European, national and international frameworks as well as on the identified material. The practices, identified during the desktop research, mostly focus on the Member State side and supplement the proposed methodology. References to these documents are available at the end of this report.

In Chapter 3, a systematic approach is provided, comprised of five steps, for the cybersecurity supply chain problem together with recommended security practices for each methodological step. It covers:

- organisational wide ICT/OT supply chain strategy;
- technical, operational and organisational measures in supply chain, considering a risk-based approach [20];
- the handling of vulnerabilities [21]; and
- the overall quality of products and cybersecurity practices (including secure development procedures) [22].

Moving forward, this report concludes by providing information for further considerations on ICT/OT supply chain.

It was identified that different terms or definitions are used in the international bibliography for similar concepts, e.g. ICT/OT supply, digital chain, third party risk management (TRM), or cyber supply chain risk management. In this report, the term ICT/OT supply chain cybersecurity is used, while a selection of definitions from policy documents is available in Annex C.

[18] ENISA, NIS Investments: November 2022. https://www.enisa.europa.eu/publications/nis-investments-2022
[19] Essential and important entities are typically operators that provide services that are considered critical to the economy and society. Essential and important entities are any entities of a type referred to in Annex I and Annex II respectively of NIS2 directive.
[20] NIS2 directive, Article 21(1).
[21] NIS2 directive, Article 21(3).
[22] NIS2 directive, Article 21(3).

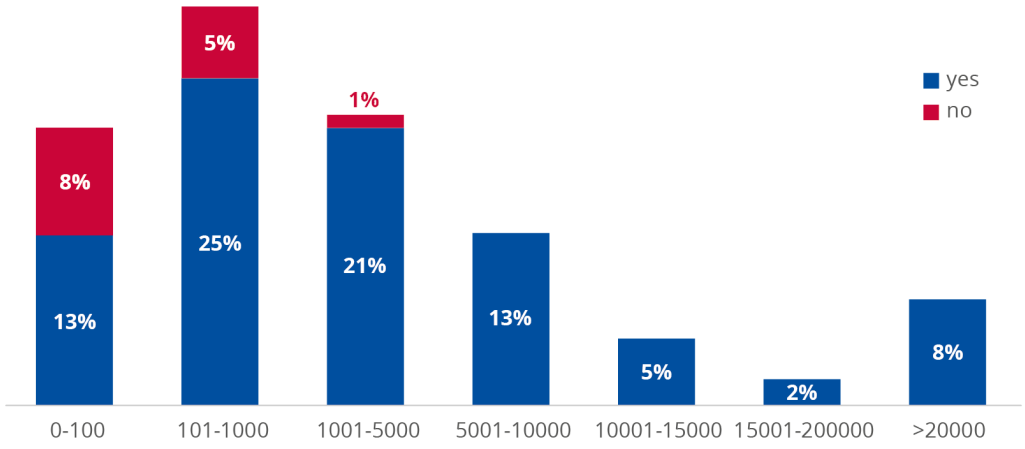
2. CURRENT PRACTICES

In an effort to provide findings and good practices for ICT/OT supply chain cybersecurity, a survey was executed by ENISA from April to June 2022 among surveyed organisations from various Member States [23]. In order to ensure adequate representation by all 27 EU Member States, a minimum of 40 organisations were surveyed per Member State. Since the survey took place before the adoption of the NIS2 directive, the surveyed organisations are operators of essential services (banking, digital infrastructure, drinking water supply and distribution, energy, financial market infrastructure, healthcare, transport sectors) or digital service providers (cloud computing, online marketplaces, online search engines).

2.1 FINDINGS

Of the surveyed organisations, 86 % have implemented ICT/OT supply chain cybersecurity policies. Only 14 % of the surveyed organisations have no approved security policies related to third parties – i.e. partners, vendors or suppliers. The survey observes that the larger the organisation, the more likely that it has such a policy in place.

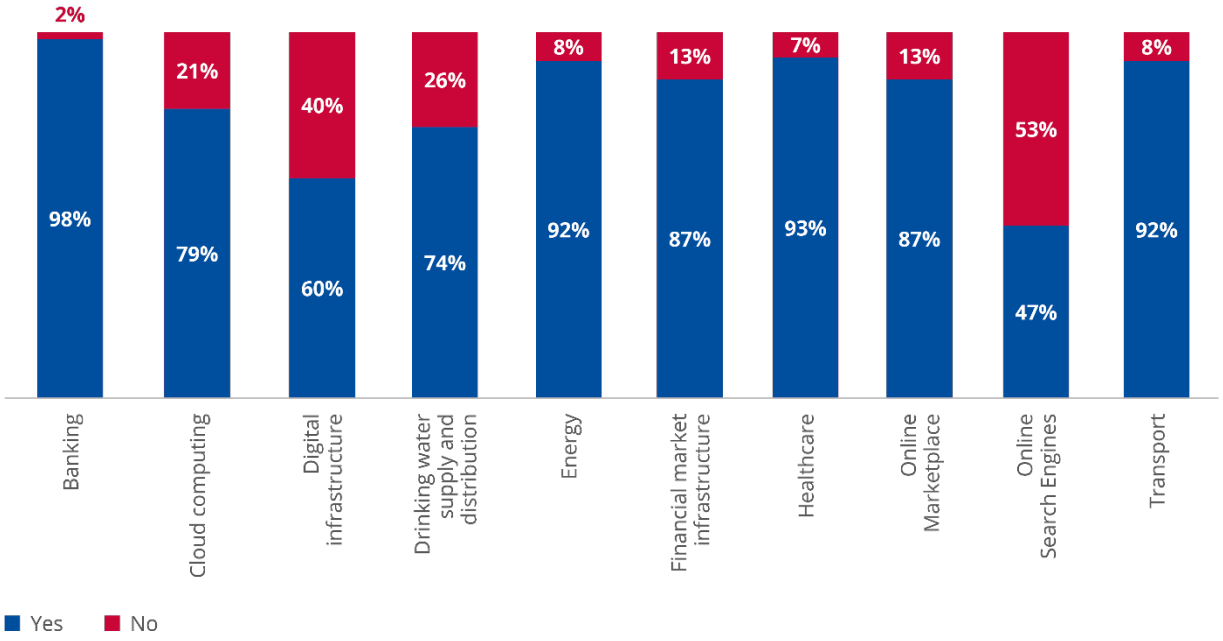
Figure 1: Approved ICT/OT supply chain cybersecurity risk management policies in place per organisation size



This was further broken down per sector, which indicated that the banking sector could be considered as the most mature when it comes to ICT/OT supply chain cybersecurity policy.

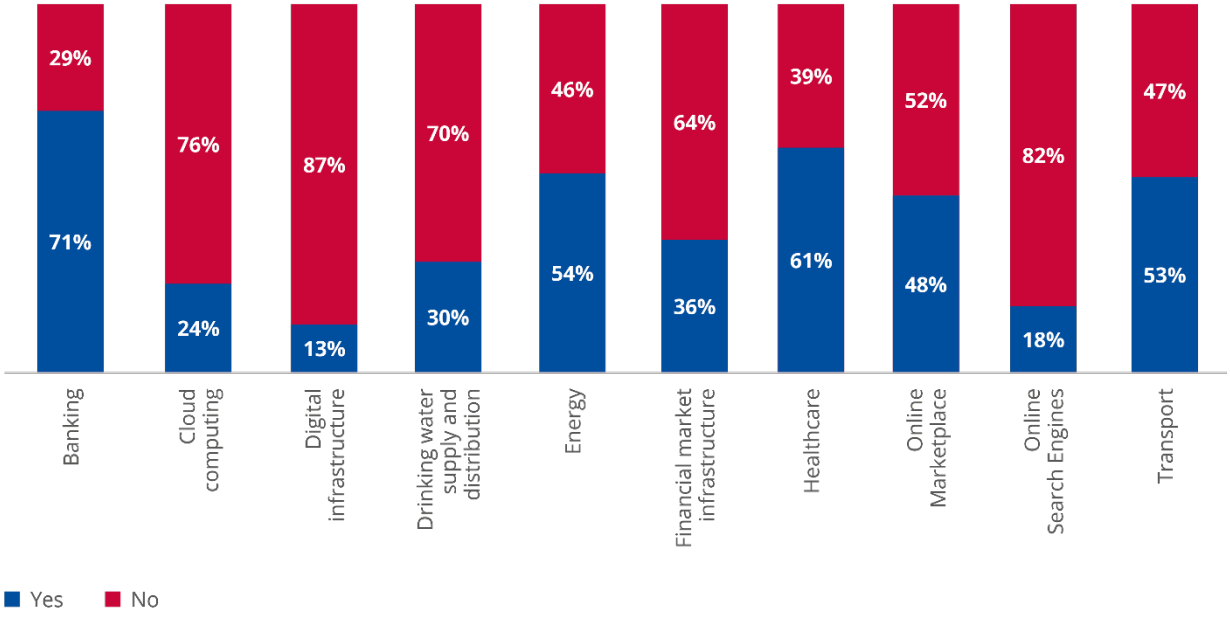
[23] See footnote 18.

Figure 2: ICT/OT supply chain cybersecurity risk management policies per sector



Despite the existence of policies, organisations do not seem to invest in ICT/OT supply chain cybersecurity. Only 47 % of the surveyed organisations in the EU have allocated budget for ICT/OT supply chain cybersecurity, whereas the majority of the surveyed organisations (53 %) do not have approved budget for such issues. The banking sector is in the lead again, with the highest percentage of dedicated ICT/OT supply chain cybersecurity budgets.

Figure 3: Dedicated ICT/OT supply chain cybersecurity budget per sector



Balancing exposure to cybersecurity risks throughout the supply chain with the costs and benefits of implementing ICT/OT supply chain cybersecurity practices and controls should be a key component of the operator's overall approach to ICT/OT supply chain cybersecurity. Enterprises should be aware that implementing ICT/OT supply chain cybersecurity practices and controls necessitates additional financial and human resources. Implementing ICT/OT

supply chain cybersecurity processes and controls requires human, tooling, and infrastructure investments, both by operators and their suppliers. However, enterprises have finite resources and as such, enterprises should carefully weigh the potential costs and benefits when making ICT/OT supply chain cybersecurity resource commitment decisions and make decisions based on a clear understanding of any risk exposure implications that could arise from a failure to commit the necessary resources to ICT/OT supply chain cybersecurity.

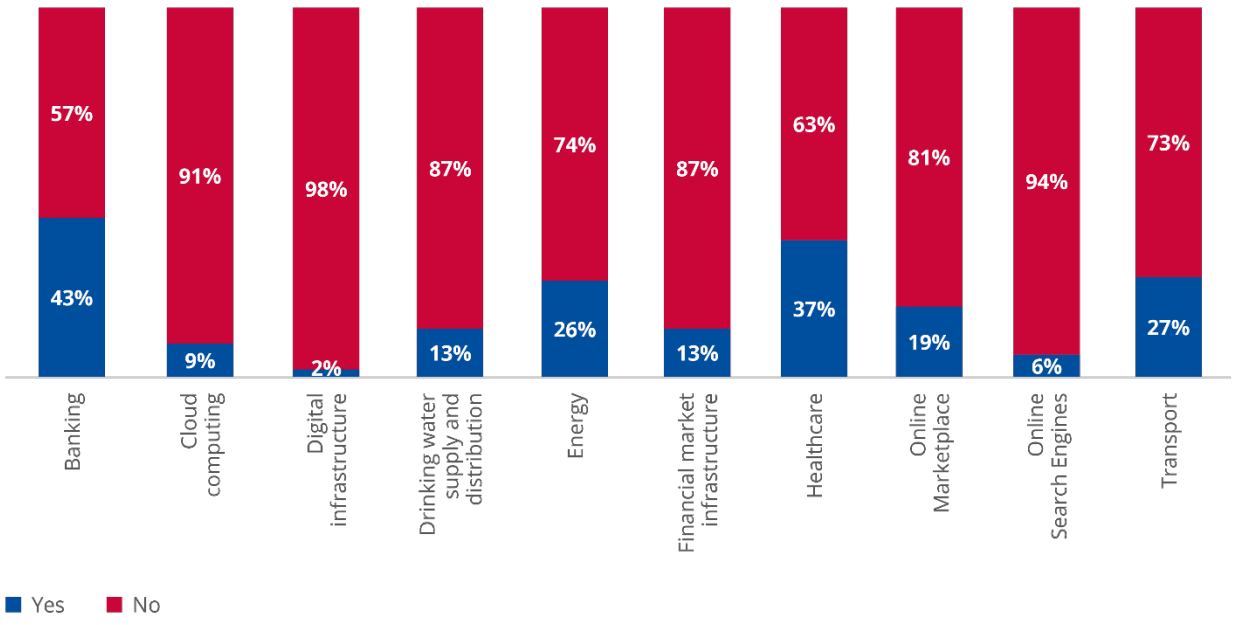
Surveyed organisations lack the necessary corporate governance structures to manage ICT/OT cybersecurity supply chain risks.

It was further identified that **only 24 % of the surveyed organisations have dedicated roles and responsibilities for ICT/OT supply chain cybersecurity.** The majority of the surveyed organisations (76 %) have no dedicated full-time equivalents (FTEs) for these matters. Also, **59 %** of **the surveyed organisations that have** TRM **policies in place also have a dedicated budget** or budget line for supply chain security.

When it comes to the respective organisation size, the medium-size organisations are the ones that predominantly have dedicated budget for supply chain security.

A further breakdown was made per sector, indicating that **the majority of surveyed organisations – regardless of the sector – do not have dedicated ICT/OT supply chain cybersecurity roles**. That being said, essential entities in the banking and healthcare sectors appear to be more likely to have such dedicated roles.

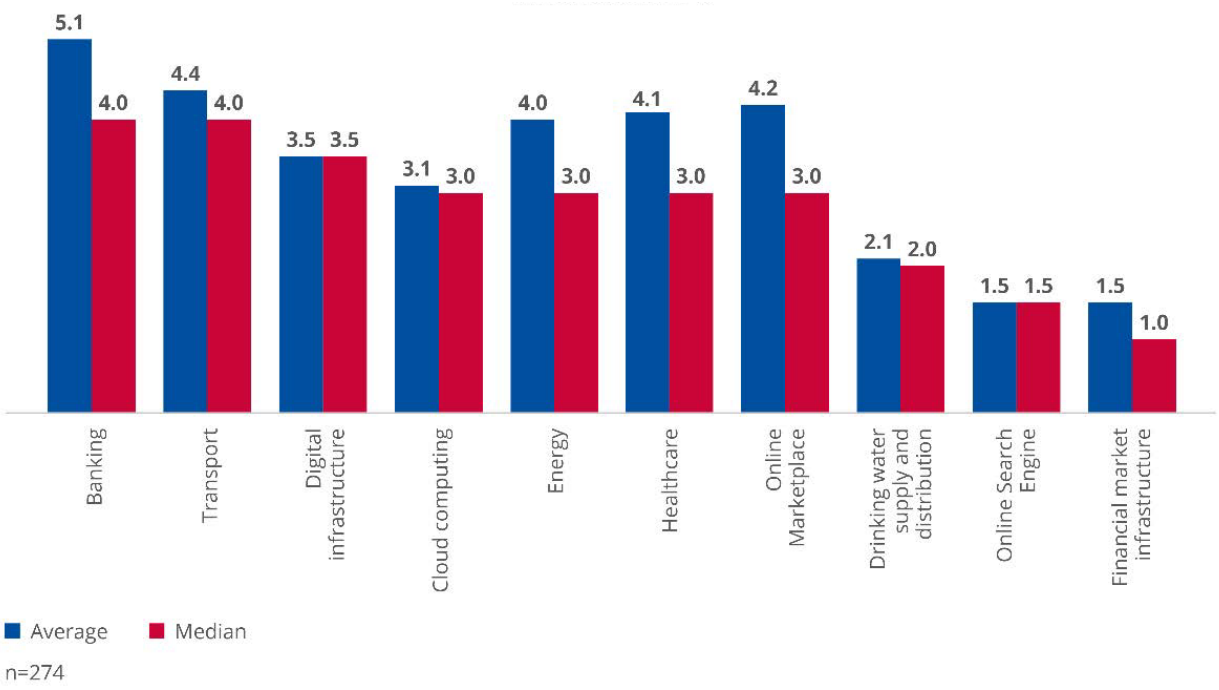
Figure 4: Dedicated ICT/OT supply chain cybersecurity role per sector



Out of the 274 organisations that have dedicated employees for ICT/OT supply chain cybersecurity, the banking sector has the highest number of ICT/OT supply chain cybersecurity FTEs, with a median value of 5 FTEs in 2021, followed by the transport and digital infrastructure sectors, with 4 and 3.5 FTEs respectively.

There is a clear indication that despite the existence of policies, operators or digital service providers lack the necessary corporate governance structures to manage ICT/OT cybersecurity supply chain risks.

Figure 5: Dedicated ICT/OT supply chain cybersecurity FTEs per sector

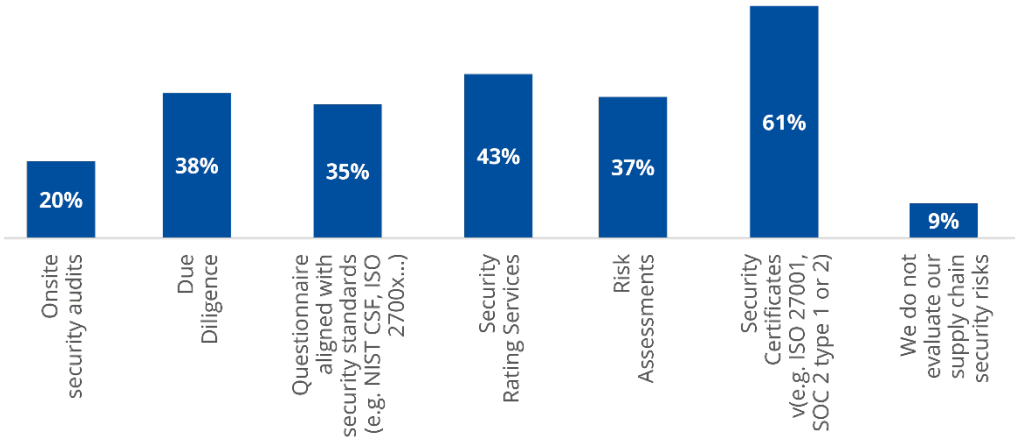


Effective ICT/OT supply chain cybersecurity requires commitment, direct involvement, and ongoing support from senior leaders and executives. Enterprises should designate the responsibility for leading organisational wide ICT/OT supply chain cybersecurity activities to an executive-level individual, office (supported by expert staff) or group (e.g. a risk board, executive steering committee or executive leadership council) regardless of the organisational structure. The exposure to cybersecurity risks might be increased for operators with inefficient or non-existent ICT/OT supply chain cybersecurity policies. The level of exposure is analogous to the criticality of the supported business process, product or service.

The supply chain may be long, with numerous tiers, or short, with few tiers. Operators with short supply chains (e.g. online search engine) might assign less FTEs to ICT/OT supply chain cybersecurity, however the NIS2 directive addresses only direct (first tier) suppliers. As a good practice, members of the ICT/OT supply chain cybersecurity team should come from different corporate functions such as information security, procurement and legal, in order to offer to the team the capacity to treat supply chain issues with a multidimensional perspective.

When asked which ICT/OT supply chain cybersecurity risk mitigation techniques were adopted, **61 % of the surveyed organisations indicated a preference for security certificates, followed closely by security risk rating services (43 %) and due diligence or risk assessments (37 %)**. Only 9 % of the surveyed organisations indicate that they do not evaluate their supply chain security risks in any way.

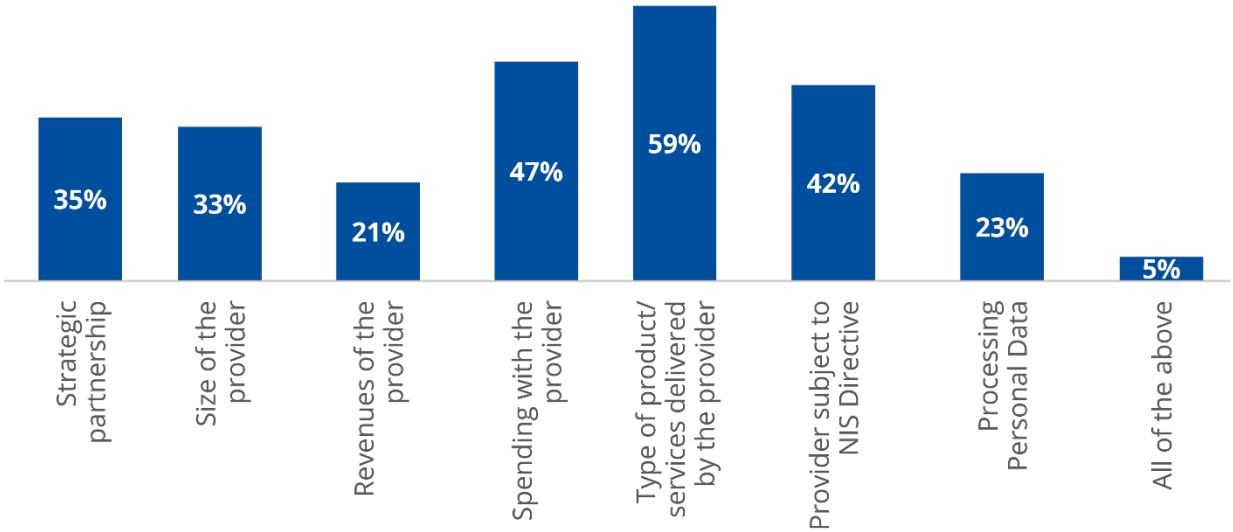
Figure 6: ICT/OT supply chain security risk mitigation techniques – all sectors



However, security certifications might be expensive, especially for smaller providers with no specialisation on cybersecurity. Requirements for a greater level of testing, documentation, or security features from suppliers will increase the price of a product or service, which may result in increased cost to the operator. This is especially true for those products and services developed for general-purpose applications and not tailored to the specific enterprise security requirements. Certification of suppliers and/or their products is only one way to respond to assessed supply chain risks. By no means should certifications of suppliers replace the constant assessment of supply chain risks by the operators. Entities should integrate into their risk management supply chain management procedures in order to constantly assess, respond and monitor the risks stemming from their supply chains.

Organisations were also surveyed about the business criteria they consider for the evaluation of cyber risks to the supply chain. As illustrated in Figure 7, when assessing supply chain security concerns, surveyed organisations focused predominantly on the type of product/service (59 %), spending with the provider (47 %) and whether or not the provider is subject to the NIS directive (42 %).

Figure 7: Business criteria for ICT/OT supply chain risk analysis



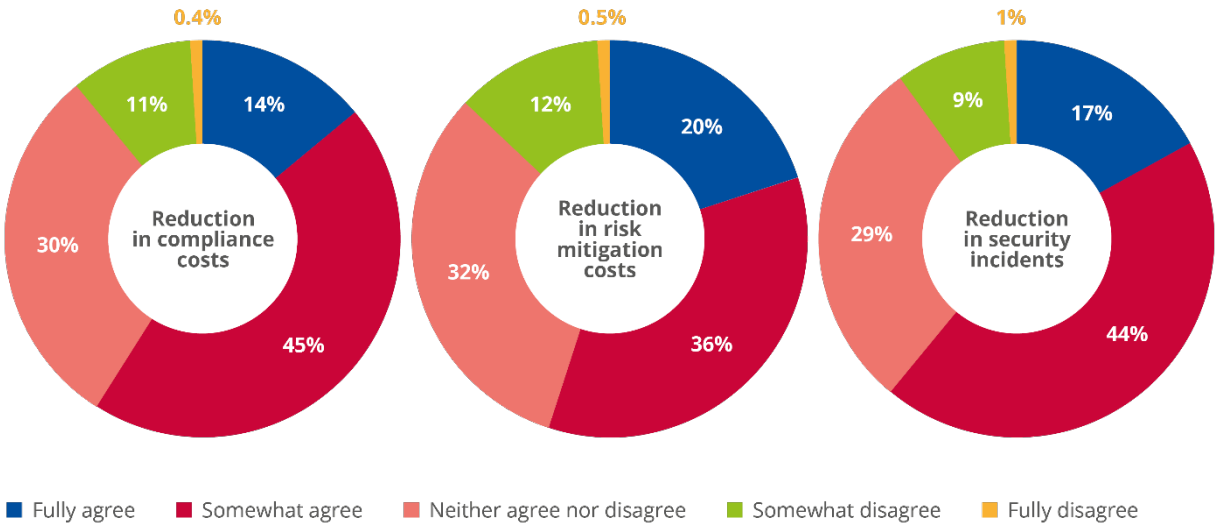
Overall, from the above figures it seems that although operators understand the cybersecurity risks stemming from the supply chain and its role in the larger ecosystem, they evaluate risks on an ad hoc basis without internally formalised capabilities for managing cybersecurity risks throughout the supply chain or capabilities to engage and share information with entities in the broader ecosystem.

When asked what the impact of potential common EU cybersecurity requirements for digital hardware and software products would be, the surveyed organisations replied as follows.

- 59 % agree that common requirements would lead to a reduction in compliance costs for users as regards their supply chain., while only 11.4 % of the surveyed organisations disagree with this statement.
- 56 % agree that common requirements would lead to lower risk mitigation costs for users, while only 12.5 % of the surveyed organisations disagree with this statement.
- 61 % agree that common requirements would reduce the number of security incidents and, as a result, the cost of managing and recovering from such incidents. Only 10 % of the surveyed organisations disagree with this statement.

The above findings prove that the adoption of the cyber resilience act (CRA) would be beneficial in order to address ICT/OT supply chain risks.

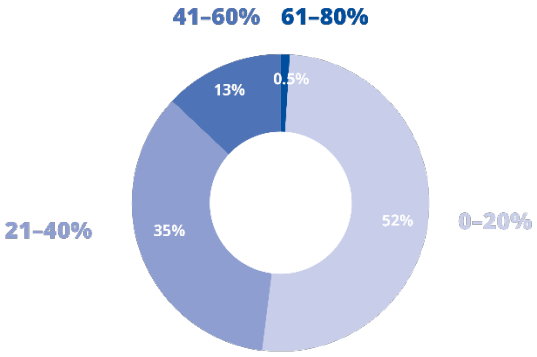
Figure 8: Perception of foreseen impact from the introduction of common EU cybersecurity requirements for digital products



Another interesting question posed was the percentage of assets over which the surveyed organisations have no visibility regarding patching. In principle, increased patching visibility results in less supply chain risks via better vulnerability management procedures. The survey data indicated that a majority of 52 % have a rigid patching policy, in which only 0 to 20 % of their assets are not covered. On the other hand, 13.5 % of the surveyed organisations have no visibility over the patching of 50 % or more of their information assets.

If asset owners cannot monitor potential vulnerabilities or receive respective vulnerability notifications from their suppliers, or if they do not understand the risks posed by product vulnerabilities in their operational context, they cannot plan and implement adequate patch management programs in order to ensure the respective risks are mitigated. However, this is not always the case according to the survey.

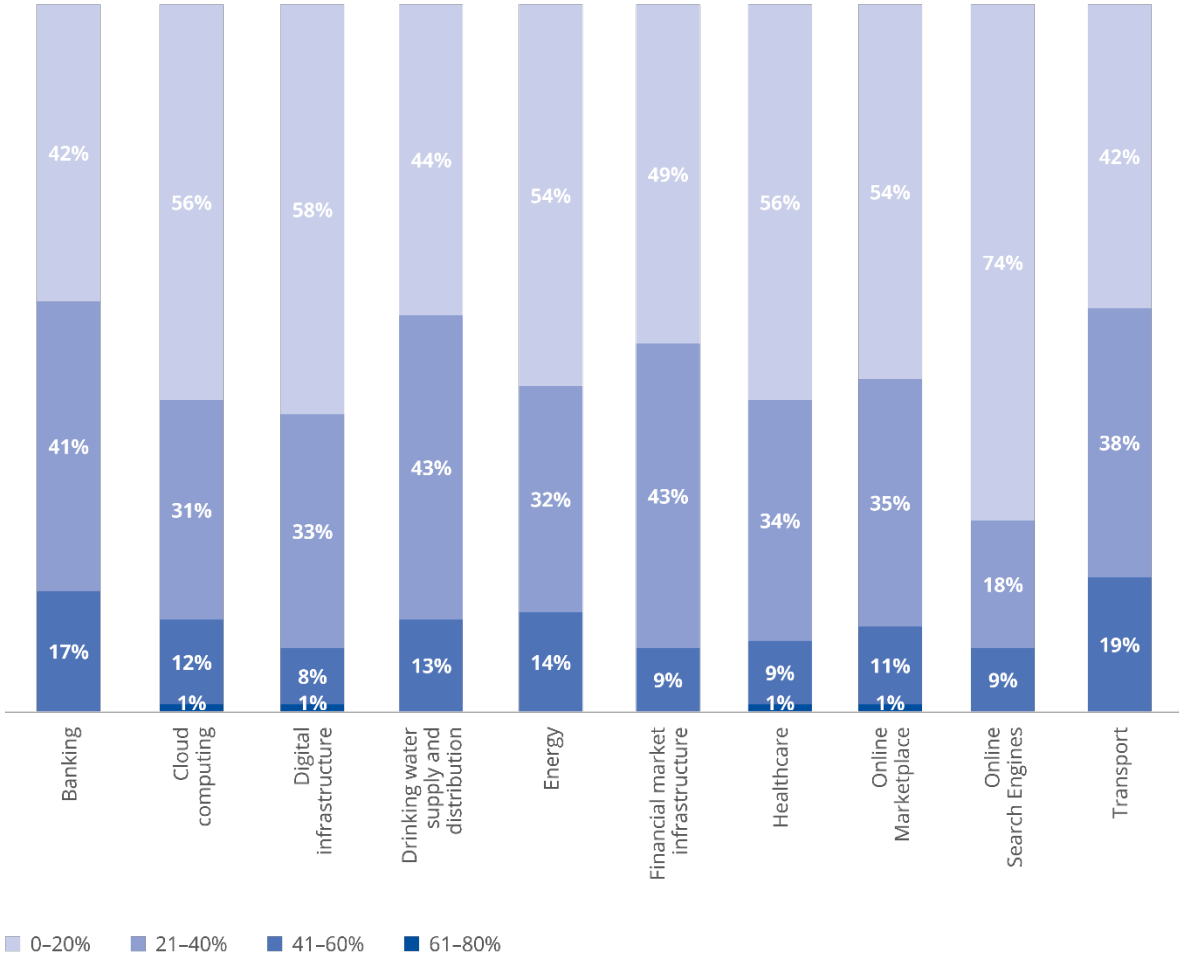
Figure 9: Visibility over the patching of assets – all sectors



1 organization answered "do not know"

As illustrated in Figure 10, a further breakdown per sector indicates similar trends across the various sectors – without any significant outliners. On the basis of the survey data, it must be noted that online search engines have the best visibility over the patching of their information assets.

Figure 10: Visibility over the patching of assets per sector



Typically, vendors of products, components and tools communicate vulnerabilities together with a patch to remediate the respective vulnerabilities. However, patching such vulnerabilities might not always be the fastest solution. While in enterprise information technology (IT) networks, standard products and tools are used, the usage of products and tools in an operational infrastructure, e.g. production plant or energy grid, patch management is not standardised.

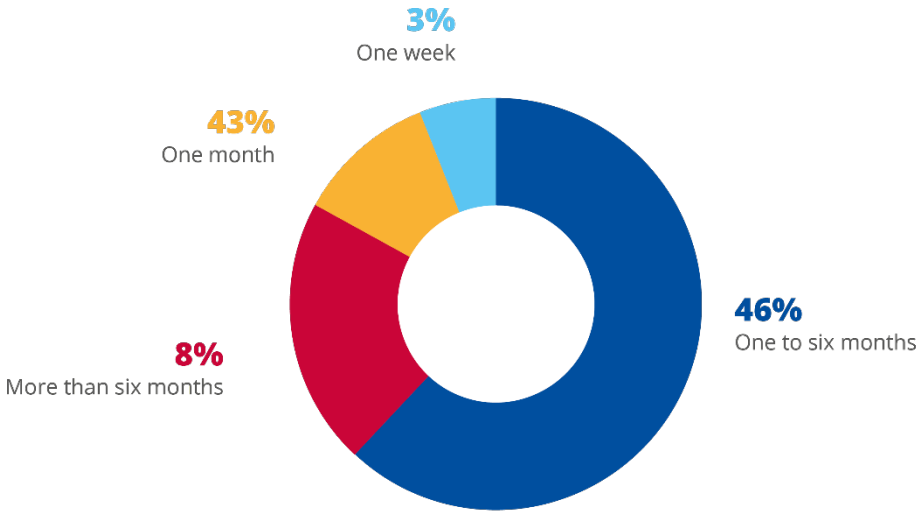
Information sharing with other operators and/or national authorities on alternative security measures would be beneficial for the deployment of a defence-in-depth strategy in order to mitigate the risks of unpatched vulnerabilities.

When asked about the normal duration of patching critical vulnerabilities on IT assets, 46 % indicated that they patch critical vulnerabilities within less than 1 month, while another 46 % indicated that they patch critical vulnerabilities within 6 months or less. As such, one may reasonably conclude that 92 % patch critical vulnerabilities at least within 6 months after their discovery.

Only 8 % of the surveyed organisations indicated that they exceed this timeline and take longer than 6 months to patch critical vulnerabilities in their systems.

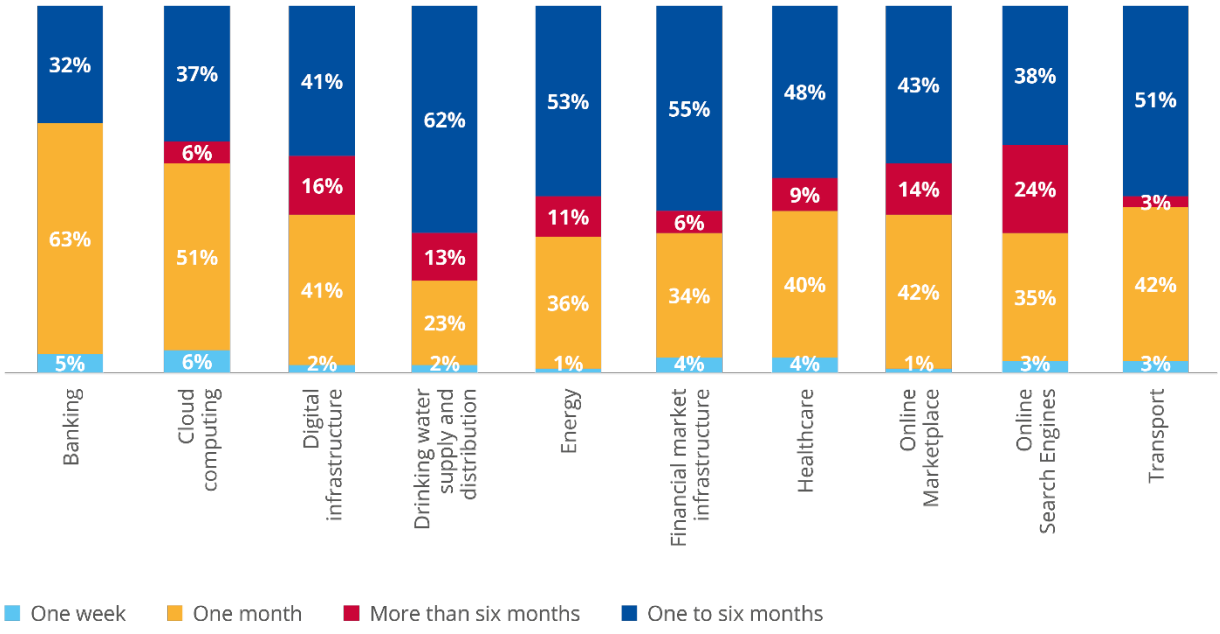
Information sharing would be beneficial for the deployment of mitigation measures for unpatched vulnerabilities.

Figure 11: Duration of patching – all sectors



As illustrated in Figure 11, a further breakdown per sector indicates that the banking sector can be considered as the best in class with regards to patching duration, while the drinking water and online search engine sectors have the longest patching duration across sectors.

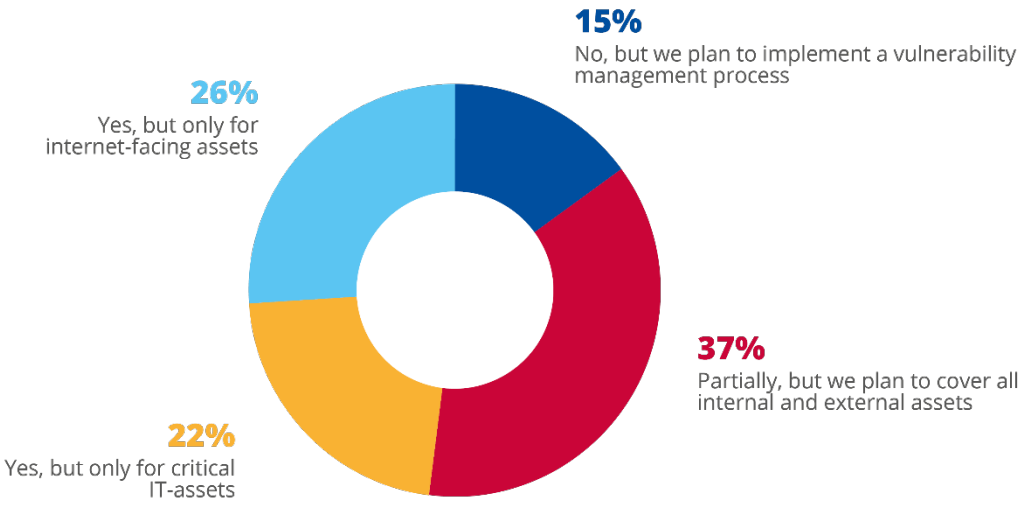
Figure 12: Duration of patching per sector



When it comes to risk-based vulnerability management processes, the survey data indicates that 48 % have implemented such a process, with 26 % only covering internet-facing assets and 22 % only covering critical assets.

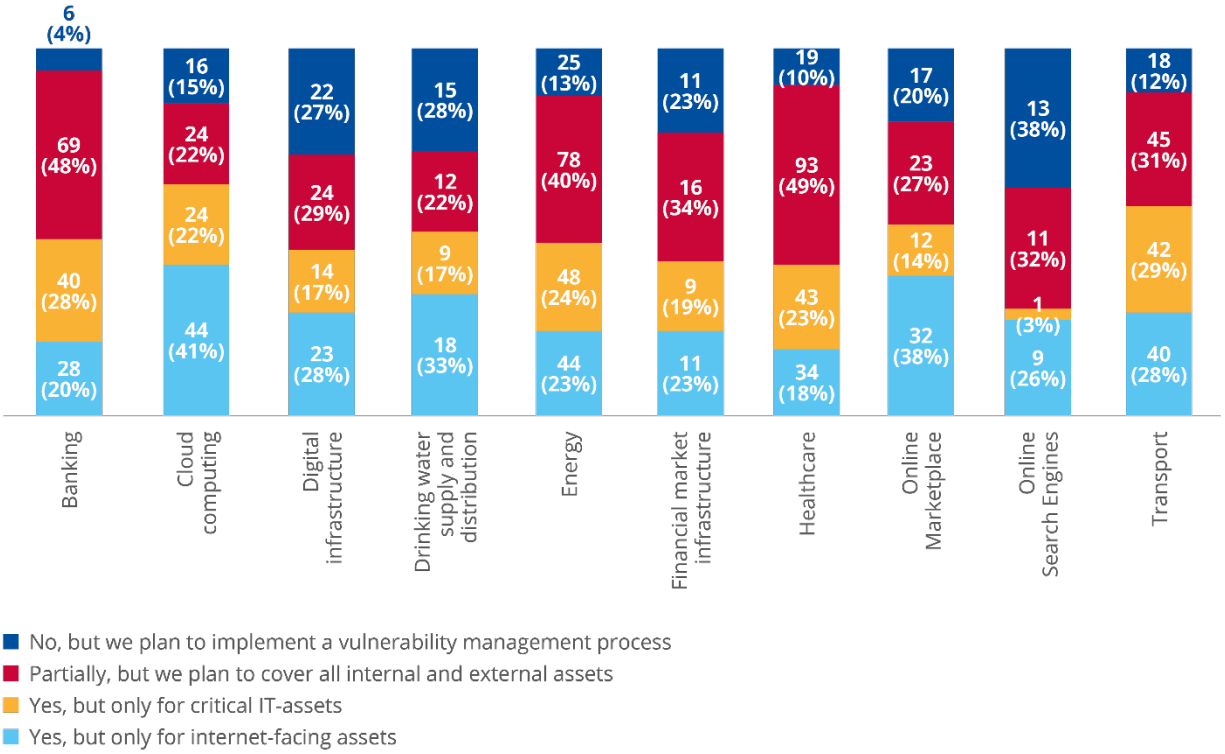
Though **37 % of the surveyed organisations have partially implemented a risk-based vulnerability management process**, it must be noted that only 15 % do not currently have such a process in place.

Figure 13: Vulnerability management – all sectors



ICT/OT supply chain cybersecurity vulnerabilities may impact operators' services as well as security. It may take a long time for such vulnerabilities to be exploited or discovered and it may also be difficult to determine whether an incident was the direct result of a supply chain vulnerability.

Figure 14: Vulnerability management per sector



Vulnerabilities in the supply chain are often interconnected and may expose operators to cascading cybersecurity risks. For example, a large-scale service outage at a major cloud service provider may lead to degradation of or disruptions to the services provided by the operator. For this reason, the operators should have a sound vulnerability management and a product testing function in place. Testing environments are required in order to adequately test the patches and at the same time avoid disruption in the operational environment.

The sector with the highest share of organisations without a risk-based vulnerability management process is the online search engine sector (38 %) whereas only 4 % of the organisations in the banking sector do not have such processes in place.

Sound vulnerability management and product testing should be in place. Testing environments are required to avoid disruption in the live environment.

2.2 SUMMARY

Putting all the abovementioned data together provides the following picture concerning the supply chain cybersecurity practices across EU:

1. Although organisations understand the significance of supply chain security, they do not allocate the necessary resources for ICT/OT supply chain cybersecurity.
2. Even when they invest in ICT/OT supply chain cybersecurity projects, the majority do it without clear governance corporate structures which ideally should take into account the costs and benefits of implementing ICT/OT supply chain cybersecurity practices and controls.
3. Organisations with formalised ICT/OT supply chain cybersecurity corporate procedures are the minority of the surveyed sample.
4. Banking is the sector with most established ICT/OT supply chain cybersecurity policies and dedicated budget and FTEs.

5. Classification of a supply chain incident as such is cumbersome due the lack of concrete criteria.
6. Certifications are the most preferred way for organisations to follow suppliers' cybersecurity practices; however, they are accompanied by high costs, especially for non-cybersecurity relevant vendors.
7. The surveyed organisations agree that common cybersecurity requirements for products and services would be beneficial for the market.
8. There is room to improve the visibility of the organisations over their information assets.
9. The majority of surveyed organisations do not have a vulnerability management system which covers all organisational assets.
10. Vulnerability management and testing of products contribute to better ICT/OT supply chain cybersecurity posture.

3. SUPPLY CHAIN CYBERSECURITY GOOD PRACTICES

The key findings from the desktop research and from the survey highlight the lack of firm corporate governance and formalised policies for the management of supplier relationships, non-coordinated approaches to the quality of products/services received and ad hoc methods for vulnerability handling. On the basis of these findings, the identified good practices and standards and the NIS2 directive's Article 21 provisions, the following five areas of focus have been identified. For each area, some good practices are proposed for consideration by stakeholders.

3.1 STRATEGIC CORPORATE APPROACH

As observed from the survey results, organisations implement supply chain policies. However, these policies do not stem from an enterprise-wide, systematic analysis of risks related to ICT/OT supply chain cybersecurity. Therefore, essential and/or important entities should first adopt a strategic approach to ICT/OT supply chain cybersecurity risk formalised through the adoption of a dedicated strategy, rooted in a continuous screening of all ICT/OT supply chain cybersecurity dependencies. The **strategy** should ensure the following.

- Practices for ICT/OT supply chain cybersecurity are established, followed, maintained and documented.
- Up-to-date policies or other organisational directives define requirements for activities on ICT/OT supply chain cybersecurity.
- Adequate resources (people, funding and tools) are provided to support ICT/OT supply chain cybersecurity activities.
- Supply chain risk teams that include executives from across the organisation (e.g. cyber, product security, procurement, legal, privacy, enterprise risk management, business units, etc.) are established (NISTIR 8276 [24]). Personnel performing activities relevant to ICT/OT supply chain cybersecurity have the skills and knowledge needed to perform their assigned responsibilities.
- Responsibility and authority for the performance of activities relevant to ICT/OT supply chain cybersecurity are assigned to personnel. Explicit collaborative roles, structures, and processes for supply chain, cybersecurity, product security, and physical security functions are created (NISTIR 8276).
- The Executive Board is increasingly involved in ICT/OT supply chain cybersecurity through regular risk discussions and sharing of measures of performance (NISTIR 8276).

Having defined the strategy, the next step is the assessment of the risks related to the cyber supply chain of the entity. The NIS2 directive, in essence, requires entities to implement a risk-based approach which '*shall ensure a level of security of network and information systems appropriate to the risk presented*'. Moreover, the survey on investments has highlighted the fact that ICT/OT supply chain cybersecurity should be done in coordinated manner. Therefore, it is recommended that entities follow a risk-based approach when trying to assess the security of their cyber supply chains via ICT/OT supply chain cybersecurity.

ICT/OT supply chain cybersecurity according to NIS2 directive needs to address the following aspects in a risk-based approach:

- supply chain risk management;
- supplier relationship of essential and important entities with different kinds of suppliers and service providers;
- vulnerability handling in products and components;
- quality of products and cybersecurity practices of suppliers and service providers.

[24] NISTIR 8276 Key Practices in Cyber Supply Chain Risk Management: Observations from industry, February 2021.

These aspects can be structured in a plan-do-check-act (PDCA) continuous improvement process. The PDCA methodology is well recognised and known from the ISO 9001 quality improvement cycle. In Figure 15, the PDCA cycle for supply chain cybersecurity is shown.

Figure 15: Cybersecurity ICT/OT Supply Chain Risk Management Cycle

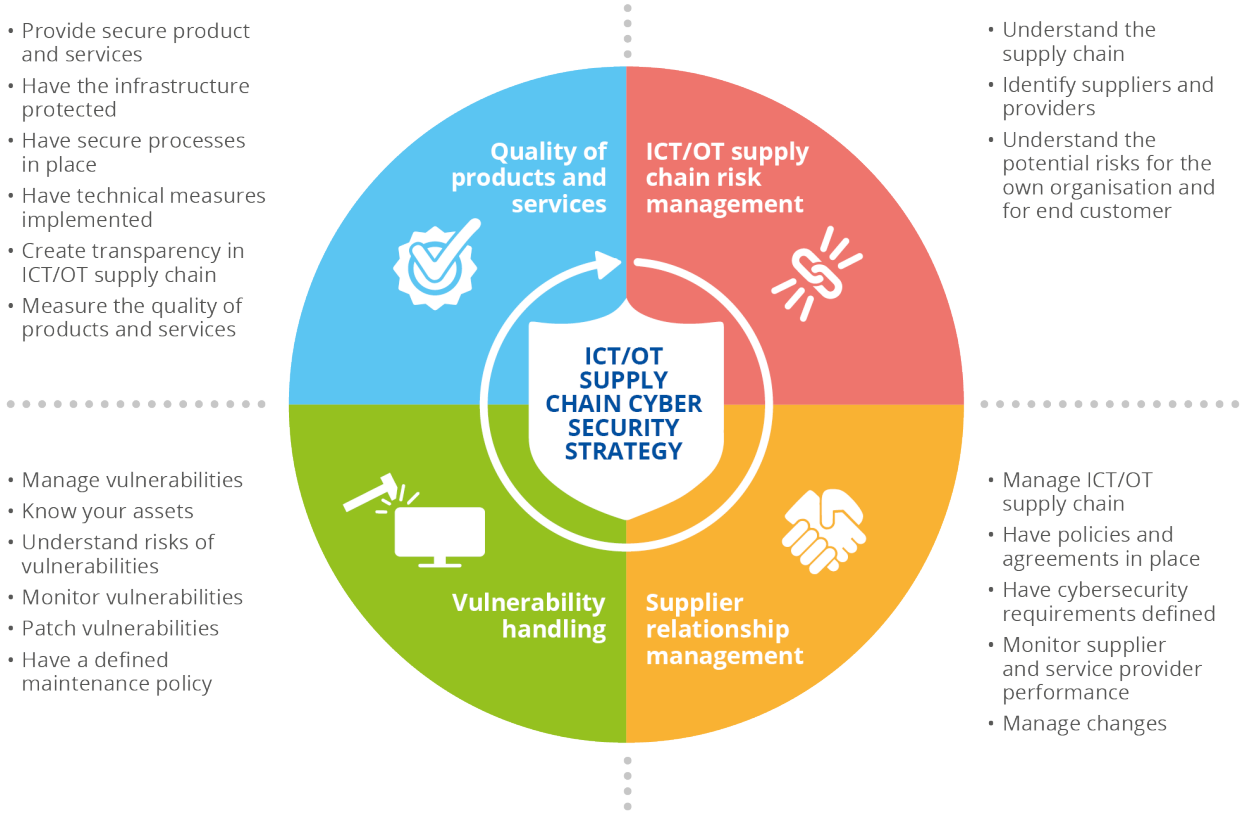


Figure 15 defines the following steps.

- It starts with the **ICT/OT supply chain risk assessment** (Section 3.2) that helps organisations to understand their respective supply chain through identification of suppliers and service providers and through understanding the potential supply chain risks for the own organisation and for end customers related to the deliverables of used suppliers and service providers.
- **Supplier relationship management** (Section 3.3) helps to manage the supply chain with policies, procedures and agreements that address supply chain risks. This is supported by monitoring of the supplier's and service provider's performance and change management practices.
- **Vulnerability handling** (Section 3.4) defines how an organisation manages vulnerabilities. Vulnerabilities of own assets are monitored and linked to assets in the infrastructure. Their risks are understood, and patches are deployed to close these vulnerabilities based on a well-defined maintenance policy.
- An important factor for supply chain cybersecurity is the **quality of products and services** (Section 3.5) used in an organisation. This requires actors along the supply value chain to implement processes with cybersecurity practices in place, to have their own infrastructure protected and technical measures in products and services implemented that increases the cyber-robustness. Quality needs to be measured and continuously improved. Essential and important entities need to have transparency on cybersecurity practices for delivered products and services.

Please note the following.

- All the abovementioned steps might be followed by both essential and important entities.
- Providers of digital services along with manufactures within the scope of the NIS2 directive might have the dual role of an essential/important entity and of a product/service supplier at the same time.
- Essential and/or important service providers might follow good practices concerning the quality of products and services for the four categories of suppliers, namely: manufacturing entities of products and components; system integrators; managed security service providers; and providers of digital services with the 'software as a service' business model.

The proposed good practices are listed in the form of tables. Substantial effort was made to link each practice as much as possible to existing standard(s). In each table of practices, references to standards have been included, where available.

3.2 SUPPLY CHAIN RISK MANAGEMENT

A risk assessment process is well documented in ISO 31000:2018 [25] which is recommended to be applied to ICT/OT supply chain risk management in regards of cybersecurity as well.

Table 2: Good practices for an ICT/OT supply chain cybersecurity risk assessment

Measure	Objective
Scope, context, criteria	
Identify and document types of suppliers and service providers [26] [27].	Understand and document the organisation's suppliers and service providers.
Identify business objectives for the own organisation and end customer's organisation.	Consider supply chain risk beyond the own organisation.
Risk criteria for different types of suppliers and services should be defined [28].	Risk criteria should reflect objectives and accepted risk level of the organisation.
Risk assessment	
Supply chain risks should be assessed in regards of own business continuity impact assessments and requirements [29].	Have business continuity requirements taken into consideration for supply chain risks.
Risk treatment	
Measures for risk treatment should be implemented with controls recommended in international standards such as ISO/IEC 27001 or ISO 9001 [30].	Apply good practices in risk mitigation which are based on international standards.
Monitoring and review	
Internal and external information resources shall be used to identify supply chain risks and threats [31].	Understand supply chain risks.
Findings from the supplier's and service provider's performance monitoring and reviews shall be considered [32].	Understand risks linked to the performance of suppliers and service providers.

Under risk criteria, the entity should follow good practices to also identify dependencies on third-party suppliers of these services and assets, making sure that:

[25] ISO 31000:2018 Risk management – Guidelines
[26] As the recommended supply chain security procedure is expected to be resource intensive, this study recommends the application be limited to critical ICT services, systems or products. The entity should determine which services will be included in the supply chain project by following an assessment methodology, e.g. impact assessment. In order to complete this exercise, the importance of the service should be assessed by taking into consideration various aspects such as the value of the information involved, the impact of the service to the business, etc. At the end of this step, a list of critical services should be in place.
[27] ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls, par. 5.19 (a).
[28] ISO 31000:2018 Risk management – Guidelines, par. 6.3.3.
[29] ISO/IEC 27031:2011 Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity.
[30] ISO/IEC 27002:2022, par. 5.22,
ISO 9001:2015 Quality management systems – Requirements.
[31] ISO 31000:2018, par. 6.4.2.
[32] ISO/IEC 27002:2022, par. 5.22.

- important IT and OT supplier dependencies are identified (i.e. external parties on which the delivery of the function depend, including operating partners);
- important customer dependencies are identified (i.e. external parties that are dependent on the delivery of the function, including operating partners);
- critical software dependencies are mapped – down to the level of packages, libraries and modules;
- single points of failure and other essential dependencies are identified.

At the end of the identification process, a list with all suppliers should be compiled. While an exhaustive list of such businesses may not be possible, the identification of those responsible for products or services with security enforcing functions, privileged access or that handle particularly sensitive information should be prioritised. A good practice for inspiration is the UK Cabinet Office's *Supplier Assurance Framework: Good practice guide* [34].

Entities shall identify and assess supplier risk as an integral component of their risk management approach, taking into account the following, among other things [33]:

- risk factors and results of EU coordinated risk assessments, if available;
- country-specific information (e.g. threat assessment from national security services etc.), if available;
- restrictions or exclusions posed by a relevant national authority, e.g. in critical equipment or for high-risk suppliers;
- information stemming from known incidents or cyber threat intelligence;
- the characteristics of each supplier, such as the quality of its security practices, the legal framework, the level of transparency and more.

Entities should perform an assessment of the risk profile of all relevant potential or existing suppliers of critical ICT/OT services, systems or products [34]. Ideally, this assessment should be done in collaboration with other entities, if they are part of the same supply chain, or in collaboration with national authorities.

Examples of detailed risk treatment good practices are described in the next section.

Once cybersecurity expectations have been established with suppliers and third parties, it is important that entities maintain the confidence that those expectations and requirements are being met or remain proportional to the risk posed by the supplier. Entities should, therefore, periodically review the ability of suppliers to meet the cybersecurity requirements that have been set.

Suppliers' risk profiles change based on new information/guidelines from national authorities, threat intelligence, state-sponsored attacks and changes to the context of the supplier.

Likewise, entities should monitor changes in the risk profile of a supplier, as the threat landscape and attack surface are constantly changing and evolving. Changes may derive from new information or guidelines from national authorities, new threat intelligence information, including state-sponsored attacks, or changes in the characteristics and the context of the supplier (e.g. legal changes, being acquired by a different organisation or adopting a new operating model).

The only way to maintain a clear picture is through periodic audits or other forms of technical assessments. Provisions for such activities should be stipulated within contracts or memorandums of understanding ('right to audit' clause) and can serve as a way to gain independent assurances of the security posture of businesses.

3.3 SUPPLIER RELATIONSHIP MANAGEMENT

The best-practice standard for management of supplier relationship is ISO/IEC 27002:2022 Chapters 5.19–5.23. It requires an asset owner (entity or organisation) to define rules for suppliers and service providers that protect the asset owner's information assets and physical assets, and defines requirements for products

[33] Examples of such measures with respect to ICT risk can be found in the Digital Operational Resilience Act (DORA).
[34] A good practice is Cabinet Office, Supplier Assurance Framework: Good practice guide, United Kingdom, May 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/707416/2018-May_Supplier-Assurance-Framework_Good-Practice-Guide.pdf

and services. Furthermore, an asset owner should monitor the performance in accordance with the contractual agreements and have change management procedures in place in case products or services evolve.

Table 3: Good practices on supplier relationship management

Measure	Objective
A process to manage suppliers and service providers over the life cycle should exist that includes at least procedures for selection and qualification of suppliers and service providers [35].	Have a defined process to select and qualify suppliers and service providers
Assets and information assets that are shared with or accessible to suppliers and service providers should be classified and labelled. Procedures for accessing and handling of classified assets should be defined [36].	Have defined security controls in place for the handling of assets and information assets
Obligations of suppliers and service providers for the protection of the organisation's information assets, and access to assets and information assets, should be agreed [37].	Have defined rules and measures for access to assets and information assets agreed with suppliers and service providers
The handling of incidents should be agreed in regards of responsibilities, notification obligations and procedures [38].	Agree on executable procedures in case of incidents
Awareness training should be given to the organisations and suppliers or service providers' personnel regarding rules of engagement and behaviour based on the level of access to the organisation's assets and information assets [39].	Have a defined policy for personnel on the protection and usage of information assets and for personnel with physical access to the organisation's infrastructure and technology available. Own and external personnel are trained and understand the policy
Have procedures for the sharing of information defined [40].	Protect information sharing, e.g. by email encryption or with encrypted shares.
Regulatory and legal requirements must be considered [41].	Consider legal and regulatory requirements such as general data protection regulation.
Condition and authorisation for access to assets and information assets [42].	Keep control of access to assets such as critical infrastructure and technology as well as of information assets.
Rules for sub-contracting and potential cascading requirements should be agreed [43].	Cascade security requirements along the supply chain
A security contact should be defined on the organisation's and supplier's / service provider's side [44].	Have a defined security contact for contractual parties defined in order to have a channel to address security issues
Security scanning of personnel for access to critical assets or information assets [45].	Have background checks or clearance available for personnel with access to critical assets and information assets
Audit right should be contractually agreed [46].	Have an audit right
Security requirements should be defined for ICT/OT products and services acquired [47].	Security requirements for products (e.g., IEC 62443 series) or services (e.g., ISO/IEC 27001:2022) should be agreed
Practices should be implemented to verify that security controls are included in delivered products or services [48].	Have an acceptance test on delivered products and services available
Assurance of suppliers and service providers that no hidden features or backdoors are knowingly included [49].	Products and services should not have hidden functions or backdoors
Procedures to handle end-of-life products, components and used tools are in place [50].	Mitigate risks of products and tools used that are not in support

[35] ISO/IEC 27002:2022, par. 5.19.
[36] ISO/IEC 27002:2022, par. 5.19, 5.20.
[37] ISO/IEC 27002:2022, par. 5.19, 5.20.
[38] ISO/IEC 27002:2022, par. 5.19, 5.20.
[39] ISO/IEC 27002:2022, par. 5.19.
[40] ISO/IEC 27002:2022, par. 5.20.
[41] ISO/IEC 27002:2022, par. 5.20.
[42] ISO/IEC 27002:2022, par. 5.20.
[43] ISO/IEC 27002:2022, par. 5.20, 5.21.
[44] ISO/IEC 27002:2022, par. 5.20.
[45] ISO/IEC 27002:2022, par. 5.20.
[46] ISO/IEC 27002:2022, par. 5.20.
[47] ISO/IEC 27002:2022, par. 5.21.
[48] ISO/IEC 27002:2022, par. 5.21.
[49] ISO/IEC 27002:2022, par. 5.21.
[50] ISO/IEC 27002:2022, par. 5.21.

Measure	Objective
Monitor service performance to verify adherence to cybersecurity requirements in agreements; this includes handling of incidents, vulnerabilities, patches, security requirements, etc. [51]	Keep the security posture maintained by having suppliers and service providers adhere to the cybersecurity requirements in agreements.
If applicable, verify that the supplier's or service provider's disaster recovery plans meet the agreed service continuity levels [52].	In the case that service continuity levels are agreed, disaster recovery plans of suppliers and service providers should be verified.
A process shall be in place to manage changes in supplier agreements, e.g. changes in tools, technologies, etc. [53]	Changes in technology or tools used by products and related life cycle services need to be managed.
A process shall be in place to manage changes in service agreements, e.g., changes in tools, technologies, etc. [54]	Changes in technology or tools used by service provider need to be managed.

The measures are applicable for all considered entities and organisations. However, the implementation of the measures will differ from organisation to organisation based on the organisational need. For example, an essential and/or important entity might apply different policies and rules for suppliers and service providers related to their enterprise IT network than to their operational (critical) infrastructure. Consequently, the measures get more detailed with the use scenarios considered.

A good practice example for point 14 'Security requirements should be defined for ICT/OT products and services acquired' can be found in the energy sector with the Bundesverband der Energie- und Wasserwirtschaft whitepaper [55], which defines requirements for ICT/OT products used in critical infrastructure. The requirements for suppliers and service providers have been derived from ISO/IEC27002:2022 and ISO/IEC 27019:2017 [56] (energy domain specific controls) requirements. Security requirements are typically domain specific and will differ depending on the purpose of a product or service or the respective organisational need.

3.4 VULNERABILITY HANDLING

Any ICT/OT product used in networks and (critical) infrastructure is built from components and software that are subject to vulnerabilities. Vulnerabilities should be managed by suppliers which eventually leads to patches that need to be applied at the product user's network or (critical) infrastructure components. Furthermore, if vulnerabilities are reported in supplied components of a product, the supplier of the product itself need to analyse the vulnerability and patch for applicability and incorporation which eventually can lead to a patch for the affected product. Software products that are running on standard operating systems like Windows or Linux require a compatibility test of operating system patches to avoid compatibility issues.

Finally, deployment of patches in operational infrastructure needs to be planned under consideration of complex roll-out and maintenance schedules. Consequently, patch deployment times differ for IT networks, which is in the range of weeks, and operational infrastructure, which is in the range of months.

Vulnerabilities are typically classified according to their potential impact and exploitability. This results in a risk potential of a vulnerability that also defines how a vulnerability is treated. Vulnerabilities for products that can be remotely exploited are typically of higher risk and should be treated with higher priority than vulnerabilities that require physical access for exploitation.

The handling of vulnerabilities has two aspects; one aspect is the monitoring of vulnerabilities which leads to an analysis on the vulnerabilities identified up to a patch delivered and deployed. The other aspect is the publishing of advisories, i.e. the vulnerability notifications. A vulnerability notification has the objective to warn product users of critical vulnerabilities and might recommend alternative mitigation measures to minimise the likelihood of an exposure. Tools

[51] ISO/IEC 27002:2022, par. 5.19, 5.22.
[52] ISO/IEC 27002:2022, par. 5.22.
[53] ISO/IEC 27002:2022, par. 5.22.
[54] ISO/IEC 27002:2022, par. 5.22.
[55] https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems-engl.pdf
[56] ISO/IEC 27019:2017 Information technology – Security techniques – Information security controls for the energy utility industry.

that support the operators as well as the developers towards this direction are the software bill of materials [57] and Vulnerability Exploitability eXchange concepts, and the Common Security Advisory Framework [58].

Table 4: Good practices for vulnerability handling for operators of IT networks and operational infrastructure

Measure	Objective
An inventory of assets should be drawn up and maintained that includes patch-relevant information [59].	Enable product users to link reported vulnerabilities to respective assets.
Information resources shall be used to identify relevant technical vulnerabilities [60].	Monitor vulnerabilities, e.g. by scanning for advisories or by receiving vulnerability information from suppliers.
Evaluate the risks of vulnerabilities for the own operational environment and have a documented and implemented maintenance policy available [61].	Understand the risk of vulnerabilities and have a maintenance policy that defines treatment depending on the risk level.
Patches should be received from legitimate sources [62].	Verify the authenticity of a software and mitigate supply chain risks.
Patches should be tested before they are installed [63].	Test compatibility and against malware.
Alternative measures should be evaluated in case patches are not available or applicable [64].	Mitigate risks with additional measures, if necessary, e.g. closing of firewall ports etc.
The patch deployment process needs to consider rollback procedures as well, e.g. an effective back-up and restoration process[65].	Ensure product availability in case a patch deployment fails by applying rollback options.

While measures for product users are well captured with recommendation on operational security of ISO/IEC 27002:2022 [66], measures for product and component development (product suppliers) are better captured by IEC 62443-4-1:2018[67].

Table 5: Good practices for vulnerability handling in product and component development

Measure	Objective
A process shall be implemented for receiving and tracking to closure of security vulnerabilities reported by internal and external sources that includes used third-party components [68].	Monitor all used components for vulnerabilities and track them for closure; the measure implicitly requires having an asset list of used third-party components maintained.
A process shall be implemented to analyse the risks of vulnerabilities in the context of the documented intended use and operational environment (if applicable) by using a vulnerability scoring system (e.g. the common vulnerability scoring system) [69].	Understand the risks of vulnerabilities by using recognised practices for vulnerability scoring.
A maintenance policy shall exist that defines the treatment of identified vulnerabilities depending on the risk [70].	Define how vulnerabilities are treated depending on the risk level.
A process shall be implemented for informing product users about vulnerabilities [71].	Inform product users on vulnerabilities.
A process shall be implemented to verify that a patch is addressing the respective vulnerability and that the patch does not contradict other operational, safety or legal constraints [72].	Patches shall be qualified before a release.

[57] https://www.cisa.gov/sbom
[58] https://docs.oasis-open.org/csaf/csaf/v2.0/csaf-v2.0.html
[59] ISO/IEC 27002:2022, par. 5.9.
[60] ISO/IEC 27002:2022, par. 8.8.
[61] ISO/IEC 27002:2022, par. 8.8.
[62] ISO/IEC 27002:2022, par. 8.8.
[63] ISO/IEC 27002:2022, par. 8.8.
[64] ISO/IEC 27002:2022, par. 8.8.
[65] ISO/IEC 27002:2022, par. 8.31.
[66] ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls.
[67] IEC 62443-4-1:2018 Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements.
[68] IEC 62443-4-1:2018, DM-1.
[69] IEC 62443-4-1:2018, DM-2, DM-3.
[70] IEC 62443-4-1:2018, DM-4, IEC 62443-4-1 SUM-5.
[71] IEC 62443-4-1:2018, DM-5, IEC 62443-4-1 SUM-2.
[72] IEC 62443-4-1:2018, SUM-1.

Measure	Objective
Check compatibility with non-built-in third-party components [73].	A compatibility test with dependent third-party products shall be maintained. A compatibility list shall be made available for all product users.
A delivery process for patches shall be implemented that verifies authenticity and integrity of a patch [74].	It shall be possible for product users to verify authenticity and integrity of delivered patches.
Documentation concerning patches shall be provided to product users that includes installation instructions and information on closed vulnerabilities [75].	Product users shall be able to understand which vulnerabilities will be closed by a patch and have installation instructions available to deploy the patch.

More guidance on vulnerability and patch management can be found in IEC TR 62443-2-3:2015 [76].

Table 6: Good practices for vulnerability handling in system integration

Measure	Objective
A system integrator shall have the capabilities for handling vulnerabilities that can affect the respective system, including related policies and procedures [77].	Select products that are supported during operating timeframe in order to have a patchable system. The system integrator shall be capable of monitoring all used products for vulnerabilities.
A documentation shall exist that describes how patches are qualified [78].	Have a defined procedure to qualify patches of products used in systems.
A procedure shall exist to document the status and applicability of patches to a system [79].	Have a documented list on available and applicable patches that can be provided to the asset owner.
The system integrator shall have the capability to deliver and install patches to the respective system [80].	Have updates provided and installed on the system to close vulnerabilities.
The system integrator shall have the capability to ensure that the hardening level is retained after patching [81].	Ensure the security level remains at a defined level.

3.5 QUALITY OF PRODUCTS AND PRACTICES FOR SUPPLIERS AND SERVICE PROVIDERS

To achieve quality in product and services, two high-level objectives apply.

1. An adequate process should be deployed that delivers the expected quality.
2. A control process should be applied to verify the efficiency of the process deployed.

This chapter will list good practices for suppliers and service providers to meet these high-level objectives.

3.5.1 Suppliers

A supplier of products should have processes in place that provide quality products in regards of cybersecurity. As an overview, it can be summarised as follows. A supplier has the infrastructure and organisation relevant for the design, development, manufacturing and delivery of products and components managed by the requirements of ISO/IEC 27001. A secure development process such as IEC 62443-4-1:2018 [82] is deployed, and technical requirements of products and components are set out in IEC 62443-4-2:2019 [83]. A quality management system ISO 9001 is implemented to continuously improve the quality.

[73] IEC 62443-4-1:2018, SUM-3.
[74] IEC 62443-4-1:2018, SUM-4.
[75] IEC 62443-4-1:2018, SUM-2.
[76] IEC TR 62443-2-3:2015 Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment.
[77] IEC 62443-2-4:2019, SP.03.03.
[78] IEC 62443-2-4:2019, SP.11.01.
[79] IEC 62443-2-4:2019, SP.11.02.
[80] IEC 62443-2-4:2019, SP.11.03, IEC 62443-2-4 SP.11.04.
[81] IEC 62443-2-4:2019, SP.11.06 RE1.
[82] IEC 62443-4-1:2018 Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements.
[83] IEC 62443-4-2:2019 Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS component.

Table 7: Good practices for suppliers

Measure	Objective
The infrastructure used to design, develop, manufacture and deliver of products and components is managed by controls of ISO/IEC 27001:2022.	Practices for cybersecurity that should be at least implemented are: — policies for information security A.5.1 — information security roles and responsibilities A.5.2 — user endpoint devices A.8.1 — remote working A.6.7 — information security awareness, education and training A.6.3 — responsibilities after termination or change of employment A.6.5 — asset management A.5.9–5.14 — access control A.5.15–5.18 — physical controls A.7 — protection from malware A.8.7 — technical vulnerability management A.8.8 — network security management A.8.20–8.23 — secure development environment A.8.25 — response to information security incidents A.5.26.
A general product development/maintenance/ support process shall be implemented that is consistent with commonly accepted product development processes [84].	Have a development, maintenance and support process implemented to ensure consistent output.
A secure development process shall be implemented that is consistent with commonly accepted security practices [85].	Practices for a secure development process should at least include: — identification of responsibilities SM-2 — custom developed components from third-party SM-10 — assessing and addressing security-related issues SM-11 — product security context SR-1 — threat model SR-2 — product security requirements SR-3 — secure design principles SD-1 — security design review SD-3 — secure coding standards SI-2 — security requirements testing SVV-1 — vulnerability handling DM-1, DM-3, DM-5 — security update qualification and delivery SUM-1, SUM-3 — security update documentation SUM -2 — security hardening and operation guidelines SG-3, SG-5.
Applicability or technical requirements based on product category and risks should be considered based on best practice standards such as IEC 62443-4-2:2019.	Standards like IEC 62443-4-2 provide a comprehensive set on security requirements which are categorised for: — requirements applicable for all products — requirements applicable for software applications (SAR) — requirements applicable for embedded devices (EDR) — requirements applicable for host devices (HDR) — requirements applicable for network devices (NDR).
Conformance statements shall be accessible for product users of essential and important entities for ISO/IEC 27001:2022, IEC 62443-4-1:2018, and IEC 62443-4-2:2019.	Conformance statements can provide transparency on implemented processes and technology for product users.
Quality objectives such as number of defects or externally identified vulnerabilities shall be defined, measured, and used as instrument to improve the overall quality [86].	Have a process defined to monitor and improve the product quality.

Please note that being selective in the controls can just provide a baseline and does not substitute an implementation of a complete process. Furthermore, referencing standards that are certifiable, offers suppliers the option to attain certification.

The standard IEC 62443-4-2 differentiates between four product categories:

[84] IEC 62443-4-1:2018, SM-1.
[85] IEC 62443-4-1:2018.
[86] ISO 9001:2015.

- Software application requirements. Software applications are pure software that typically run on host devices. Open-source software is part of this category, too.
- Embedded device requirements. An embedded device is typically a device that has a well-defined intended use and is not using standard hardware like PCs or servers. Examples of an embedded device are an intelligent electronic device that has processing and control logic functions included or a programmable logic controller that has a control logic programmed which processes data.
- Host device requirements. A host device is defined as workstations or databases. Examples are PCs, servers which are running commercial off-the-shelf operating systems like Windows or Linux and Structured Query Language database applications.
- Network device requirements. A network device is defined as a component that links multiple network segments or network nodes together or that terminates virtual private networks. Examples of such devices are switches and routers.

It should be noted that it is not possible to have a clear border between product categories and that there will always be examples where it will be difficult to categorise a product.

3.5.2 System integrators

A system integrator should have processes in place which ensure that cybersecurity requirements for systems are taken into consideration. As an overview, it can be summarised as follows. A system integrator has the infrastructure and organisation relevant for the design and deployment of a system managed by requirements of ISO/IEC 27001:2022. A secure integrator process such as IEC 62443-2-4:2019 [87] is employed, and technical requirements of the system are reflected by IEC 62443-3-3 [88]. A quality management system ISO 9001:2015 is implemented to continuously improve the quality.

Table 8: Good practices for system integrators

Measure	Objective
The infrastructure used to design and deploy a system conforms to ISO/IEC 27001:2022.	Practices for cybersecurity that should be at least implemented are: — policies for information security A.5.1 — information security roles and responsibilities A.5.2 — user endpoint devices A.8.1 — remote working A.6.7 — information security awareness, education and training A.6.3 — responsibilities after termination or change of employment A.6.5 — asset management A.5.9-5.14 — access control A.5.15 – 5.18 — physical controls A.7 — protection from malware A.8.7 — technical vulnerability management A.8.8 — network security management A.8.20-8.23 — secure development environment A.8.25 — response to information security incidents A.5.26.
A general system engineering process shall be implemented that is consistent with commonly accepted system engineering processes [89].	Have a system engineering process implemented to ensure consistent output.

[87] IEC 62443-2-4:2019.
[88] IEC 62443-3-3:2013 Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels.
[89] ISO/IEC/IEEE 15288:2015 Systems and software engineering – System life cycle processes.

Measure	Objective
A secure engineering process shall be implemented that is consistent with commonly accepted security practices [90].	Practices for a secure development process should at least include: — security responsibilities in system SP.01.06 — robustness of security tools and software SP.02.02 RE3 — hardening guidelines SP.02.03 — risk assessment SP.03.01 — network design SP.03.02 — vulnerability handling and Patch management SP.03.03, SP.11.01,SP.11.02, SP.11.03, SP.11.04, SP.11.06 — access control, session lock SP.03.06, SP.03.07 — encryption to protect data, least privilege SP.03.08 — data protection SP.03.10 — network design for wireless SP.04.02 — risk assessment for safety functions SP.05.01 — network design SP.06.01 — remote access SP.07.01, SP.07.04 — event management SP.08.01, SP.08.02 — account management SP.09.01, SP.09.03, SP.09.05 — malware protection SP.10.01, SP.10.05 — backup/restore SP.12.01, SP.12.02.
Applicability or technical requirements shall be considered based on best practice standards such as IEC 62443-3-3:2013.	Standards like IEC 62443-3-3:2013 provide a comprehensive set of security requirements which should be considered in system design.
Conformance statements shall be accessible for system users of essential and important entities for ISO/IEC 27001:2022, IEC 62443-2-4:2019, and IEC 62443-3-3:2013.	Conformance statements can provide transparency on implemented processes and technology for system users.
Quality objectives such as number of defects shall be defined, measured, and used as instrument to improve the overall quality [91].	Have a process defined to monitor and improve the delivery quality.

Please note that being selective in the controls can just provide a baseline and does not substitute an implementation of a complete process. Furthermore, referencing standards that are certifiable, offers system integrators the option to attain certification.

3.5.3 ICT Service management providers

An ICT service management provider might can offer the following.

a) Consultancy: e.g. enterprise architecture analysis, security audits, penetration testing.
b) Managed services: e.g. business continuity, incident response services.

While the focus in category (a) lies purely in competences, knowledge and experience, the focus in category (b) also has infrastructure and operational aspects. The infrastructure and operational aspects are comparable with the recommendations as pointed out for providers of digital services (see next section) and shall not be repeated here.

Table 9: Good practices for consultancy

Measure	Objective
Technical and cybersecurity experts and consultants should have competences, knowledge, and experience in the field of activity that can be categorised in a defined metric [92].	Have a defined level of expertise available.
Technical and cybersecurity experts and consultants in a specific business domain should have working experience in the respective domain [93].	Ensure that security services do not cause operational issues.

[90] IEC 62443-2-4:2019.
[91] ISO 9001:2015.
[92] NISTIR 8276.
[93] NIST SP 800-161r1.

Measure	Objective
Consultants for management systems and standards should be certified in accordance with audit requirements of respective standards [94].	Ensure that consultants are qualified.
Consultancy should consult technology neutrally and reflect good practices as defined in international standards.	Mitigate the risks of consultative selling and lack of service quality.
Have defined quality criteria implemented for services delivered by external parties [95].	External technical and cybersecurity experts and consultants are qualified and managed.
Quality objectives shall be defined, measured, and used as instrument to improve the service quality [96].	Have a process defined to monitor and improve the service quality.

3.5.4 Provider of digital services

A provider of digital services with a software as a service (SaaS) business model should have processes in place that provide quality of services. As an overview, it can be summarised as follows. A digital service provider provides services typically on a hosted infrastructure (not in focus here). The organisation own infrastructure is managed by requirements of ISO/IEC 27001. Best practice security controls from the Cloud Control Matrix (CCM) are considered. A quality management system ISO 9001 is implemented to continuously improve the service quality. It is also noted that relevant measures are included in the *Cloud Computing Compliance Controls Catalogue (C5)* [97], the SecNumCloud repository [98] and the candidate EU cybersecurity certification scheme for cloud services [99].

Table 10: Good practice for providers of digital services with a SaaS business model

Measure	Objective
The infrastructure of the own organisation is managed by controls of ISO/IEC 27001:2022.	Practices for cybersecurity that should be at least implemented are: — policies for information security A.5.1 — information security roles and responsibilities A.5.2 — user endpoint devices A.8.1 — remote working A.6.7 — information security awareness, education and training A.6.3 — responsibilities after termination or change of employment A.6.5 — asset management A.5.9–5.14 — access control A.5.15–5.18 — physical controls A.7 — protection from malware A.8.7 — technical vulnerability management A.8.8 — network security management A.8.20–8.23 — secure development environment A.8.25 — response to information security incidents A.5.26.
The environment (if applicable) is protected state-of-the-art [100].	Use cloud services from a trusted infrastructure as a service provider.
A general service process shall be implemented that is consistent with commonly accepted practices [101].	Have a service process or relevant practices implemented.

[94] NIST SP 800-161r1.
[95] ISO/IEC 27001:2022, A.5.19-5.23.
[96] ISO 9001:2015.
[97] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/ComplianceControlsCatalogue-Cloud_Computing-C5.pdf?__blob=publicationFile&v=3
[98] https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud-referentiel-exigences-v3.2.pdf
[99] https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme
[100] ISO/IEC 27002:2022, 5.23.
[101] ISO/IEC 20000-series, ITIL.

Measure	Objective
Applicable cybersecurity practices of the CCM are implemented [102].	Practices should at least include: — application and interface security AIS — business Continuity Plan and Testing BCR-01, BCR-02 — business Continuity Impact Analysis BCR-09 — change Control & Configuration Management CCC-01 — data Security & Information lifecycle management DSI — encryption & key management EKM — governance and risk management GRM-01, GRM-02, GRM-04 — human resource background screening HRS-02 — identity & Access management IAM — infrastructure & Virtualisation Security IVS — interoperability & Portability IPY — mobile security MOS — security incident management SEF — supply chain security STA — threat and vulnerability management TVM.
Conformance statements shall be accessible for service users of essential and important entities for ISO/IEC 27001:2022, CSA-CCM [103].	Conformance statements can provide transparency on implemented processes and technology for service users.
Quality objectives such as number of external reported security issues shall be defined, measured, and used as instrument to improve the overall quality [104].	Have a process defined to monitor and improve the service quality.

Many CCM requirements are potentially already addressed by ISO/IEC 27002 requirements, however the CCM offers a view which focuses on cloud applications and is well recognised.

Please note that being selective in the controls can just provide a baseline and does not substitute an implementation of a complete process. Furthermore, referencing standards that are certifiable offers suppliers the option to attain certification.

[102] CSA CCM https://cloudsecurityalliance.org/research/cloud-controls-matrix/
[103] See footnote 103.
[104] ISO 9001:2015.

4. CHALLENGES

Based on the information collected from the literature and the market, this study has identified the following issues and good practices to address ICT/OT supply chain cybersecurity.

Terminology. A significant challenge stems from terminology, since various definitions were identified in all the reviewed documents. These refer to supply chain cybersecurity and what it entails, but also to the various entities involved in the supply chain, e.g. managed service provider. This situation creates confusion, especially concerning the scope of each different approach. It also makes the comparison of these approaches challenging. This confusion around terminology is also reflected in national policy documents and can pose challenges for NIS2 directive's implementation. Therefore, efforts to create a common understanding in the scope of ICT/OT supply chain management should be undertaken.

Limitations of good practices/standards. The good practices described in this report provide the way to identify and manage supply chain cybersecurity risks for essential and important entities under the NIS2 directive. Recent supply chain attacks were the result of gaps, which could have been avoided if the recommended cybersecurity practices had been in place, both on the supplier and the customer side. The practices described in this document can contribute to an improvement in cybersecurity in the supply chain, but not all supply chain risks can be mitigated just by implementing good practices. In particular, hidden functions and undocumented access capabilities (backdoors) in hardware components cannot be exhaustively identified by the most common certifications or standard penetration tests.

Risks at the Member State level. State-sponsored attacks relate to malicious actors utilising sophisticated means with extended resources, domain specific skills and high motivation [105]. Such risks require advanced risk management capabilities, which may be difficult for an entity to acquire. They may require risks to be managed at the Member State level, e.g. with intelligence services being involved. These risks may be addressed as part of overall national policies, such as performing risk assessment for ICT/OT supply chain risks at the Member State level. Such assessments take into account known state actors in order to derive measures on sourcing from critical product suppliers and service providers.

Information sharing. Zero-day vulnerabilities which are still unpatched, i.e. vulnerabilities known only to and utilised by a specific group (e.g. a Member State), have the potential to be used by malicious groups too. Consequently, sharing information on those zero-day vulnerabilities amongst Member States might be considered a good practice in this regard.

Testing and assurance. As has been observed, a big part of supply chain cybersecurity refers to the quality of products and services. As essential and important entities provide services which are critical for society to function, testing of critical assets of their infrastructures should be an integral part of purchasing equipment and it should be encouraged and promoted by the Member States. A good practice for quality of services and products for public sector's research and development projects might be the recent concept of pre-commercial procurement (see Section 3.5).

Shared testing platforms. ICT/OT security testing is now considered so crucial that several countries have already started to work in this direction in public or private initiatives. Most of these initiatives have a geographic impact restricted to a single country or a few countries. Many of the stakeholders consider that exclusive public funding models are insufficient to achieve self-maintenance of a national or regional testing platform and that there is no reason not to include private investments if mutually beneficial. Due to the fact that every industry has its specific testing needs as well as cost for the equipment, the option of creating shared sector specialised platforms becomes financially sustainable.

[105] Based on the definition of security level 4, IEC 62443-3-3:2013.

REFERENCES

Documents used for the analysis

US Cybersecurity and Infrastructure Security Agency, 'Protecting against cyber threats to managed service providers and their customers', Alert (AA22-131A)
https://www.cisa.gov/uscert/ncas/alerts/aa22-131a

Cutter Business Technology Journal, Vol. 33, No 5, Cutter Consortium, 2020.
https://www.cutter.com/sites/default/files/itjournal/2020/cbtj2005c.pdf

US Cybersecurity and Infrastructure Security Agency, Cyber Security Procurement Language for Control Systems, September 2009
https://www.cisa.gov/sites/default/files/2023-01/Procurement_Language_Rev4_100809_S508C.pdf

ENISA, 'Threat landscape for supply chain attacks', July 2021
https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

ENTSO-e, 'Network Code for cybersecurity aspects of cross-border electricity flows', January 2022
https://eepublicdownloads.entsoe.eu/clean-documents/Network %20codes %20documents/NC %20CS/220114_NCCS_Legal_Text.pdf

EU Digital Operational Resilience Act (DORA), November 2022
https://data.consilium.europa.eu/doc/document/PE-41-2022-INIT/en/pdf

Position of the European Parliament adopted at first reading on 10 November 2022 with a view to the adoption of Directive (EU) 2022/... of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
https://www.europarl.europa.eu/doceo/document/TA-9-2022-0383_EN.pdf

Financial Industry Regulatory Authority, 'Regulatory notice: Vendor management and outsourcing', 13 August 2021
https://www.finra.org/sites/default/files/2021-08/Regulatory-Notice-21-29.pdf

Hodge, R., Martin, R. A. and Aisenberg, M., MITRE, 'Supply chain security – It's everyone's business', July 2021
https://www.mitre.org/sites/default/files/2021-10/pr-21-2015-supply-chain-security-its-everyones-business.pdf

Martin, R. A., MITRE, 'Trusting our supply chains – A comprehensive data-driven approach', January 2021
https://www.mitre.org/sites/default/files/2021-11/prs-20-01465-37-trusting-our-supply-chains-comprehensive-data-driven-approach.pdf

US National Telecommunications and Information Administration, *Roles and Benefits for SBOM Across the Supply Chain*, 8 November 2019
https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf

Czech National Cyber and Information Security Agency (NÚKIB), *National cyber security strategy of the Czech Republic for the period from 2021 to 2025*, March 2021
https://nukib.cz/en/cyber-security/strategy-action-plan/

NÚKIB, 'The recommendation for assessing the trustworthiness of technology suppliers of 5G networks in the Czech Republic', February 2022

https://www.nukib.cz/en/infoservis-en/news/1805-the-recommendation-for-assessing-the-trustworthiness-of-technology-suppliers-of-5g-networks-in-the-czech-republic/

Swedish Civil Contingencies Agency, *Digital Supply Chains Under Threat: 50 recommendations to strengthen societal security*, May 2022
https://rib.msb.se/filer/pdf/29988.pdf

UK Finance, 'UK Finance Supplier Assurance Framework', March 2022
https://www.ukfinance.org.uk/policy-and-guidance/guidance/uk-finance-supplier-assurance-framework

UK National Cybersecurity Centre, 'Secure development and deployment guidance', November 2018
https://www.ncsc.gov.uk/collection/developers-collection

Further reading

Energy Sector Control Systems Working Group, *Cybersecurity Procurement Language for Energy Delivery Systems*, April 2014
https://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf

Danish Centre for Cyber Security, *Effective Cyber Defence*, October 2021
https://www.cfcs.dk/globalassets/cfcs/dokumenter/vejledninger/en/cfcs-effective-cyber-defence.pdf

ENISA, 'NIS investments 2022', November 2022
https://www.enisa.europa.eu/publications/nis-investments-2022

KPMG, *Third-Party Risk Management Outlook 2022: Time for action*, 2022
https://assets.kpmg/content/dam/kpmg/xx/pdf/2022/01/third-party-risk-management-outlook-2022.pdf

NÚKIB, 'Warning', March 2022
https://www.nukib.cz/download/aktuality/en_2022-03-21_warning.pdf

NÚKIB, 'Warning', May 2022
https://www.nukib.cz/download/publications_en/30-05-2022_warning.pdf

Oesterreichs Energie and Bundesverband der Energie- und Wasserwirtschaft, *Whitepaper Requirements for Secure Control and Telecommunication Systems*, May 2018
https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems-engl.pdf

WEF, *Advancing Cyber Resilience: Principles and tools for boards*, January 2017
https://www.weforum.org/whitepapers/advancing-cyber-resilience-principles-and-tools-for-boards/?DAG=3&gclid=EAIaIQobChMI7_mm8-Pp-wIVCuR3Ch2qdwyYEAAYASAAEgK1EPD_BwE

WEF, *Advancing Supply Chain Security in Oil and Gas: An industry analysis*, August 2021
https://www.weforum.org/whitepapers/advancing-supply-chain-security-in-oil-and-gas-an-industry-analysis

WEF, *Cyber information sharing: Building collective security*, October 2020
https://www3.weforum.org/docs/WEF_Cyber_Information_Sharing_2020.pdf

WEF, *Cyber Resilience in the Electricity Ecosystem: Playbook for boards and cybersecurity officers*, June 2020
https://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem_Playbook_for_Boards_and_Cybersecurity_Officers_2020.pdf

WEF, *Cyber Resilience in the Electricity Ecosystem: Principles and guidance for boards*, February 2019
https://www.weforum.org/whitepapers/cyber-resilience-in-the-electricity-ecosystem-principles-and-guidance-for-boards/?DAG=3&gclid=EAIaIQobChMImvDht-Tp-wIVD9Z3Ch3gUgcOEAAYASAAEgJoKPD_BwE

WEF, *Cyber Resilience in the Electricity Ecosystem: Securing the value chain*, November 2020
https://www.weforum.org/whitepapers/cyber-resilience-in-the-electricity-ecosystem-securing-the-value-chain

WEF, *Cyber Resilience in the Oil and Gas Industry: Playbook for boards and corporate officers*, May 2021
https://www.weforum.org/whitepapers/cyber-resilience-in-the-oil-and-gas-industry-playbook-for-boards-and-corporate-officers/?DAG=3&gclid=EAIaIQobChMIrun6vuTp-wIVhK13Ch2ggQYREAAYAiAAEgLOYfD_BwE

WEF, 'Cyber risk and corporate governance', 2021
https://www.weforum.org/projects/cyber-risk-leadership-and-corporate-governance

WEF, *Cybercrime Prevention Principles for Internet Service Providers*, January 2020
https://www.weforum.org/reports/cybercrime-prevention-principles-for-internet-service-providers/

WEF, *Global Cybersecurity Outlook 2022*, January 2022
https://www.weforum.org/reports/global-cybersecurity-outlook-2022/

WEF, Partnership against Cybercrime, November 2020
https://www3.weforum.org/docs/WEF_Partnership_against_Cybercrime_report_2020.pdf

WEF, *Principles for Board Governance of Cyber Risk*, March 2021
https://www3.weforum.org/docs/WEF_Cyber_Risk_Corporate_Governance_2021.pdf

ANNEX A: RECENT SUPPLY CHAIN ATTACKS

Several cyberattacks on the supply chain have been published recently[106].

Table 11: Recent cyberattacks on the supply chain

Incident	Date	Description	Impact
SolarWinds	December 2020	SolarWinds Orion is a network management system, which was compromised in a major supply chain attack.	The attack led to a severe data breach that penetrated thousands of organisations globally [107] [108]. The investigation disclosed severe flaws in the security implementation of SolarWinds [109].
Ledger	July 2020	Attackers obtained valid credentials to access Ledger's e-commerce database [110].	The stolen data was released publicly in an online forum and was also used by the attackers for phishing and extortion of users [111]. The data was also used for stealing users' money through a physical attack after providing users with counterfeit Ledger wallets which, when connected to a computer that would ask users for their security keys, would infect the computer with malware and send the stolen information back to the attackers [112].
Mimecast	January 2021	After the supplier was compromised [113], a Mimecast-issued certificate used by customers to access Microsoft 365 services was accessed by attackers.	Attackers were able to intercept the network connections and to connect to the Microsoft 365 accounts to steal information [114].
Kaseya	July 2021	A zero-day vulnerability in Kaseya's systems was exploited, which enabled the attackers to remotely execute commands on the Virtual System/Server	Since Kaseya can distribute remote updates to all VSA servers, on 2 July 2021, an update was distributed to Kaseya's clients' VSA that executed code from the attackers. This malicious code in turn deployed ransomware [116].

[106] These incidents originate from ENISA annual threat landscapes.
ENISA, Threat Landscape for Supply Chain Attacks: July 2021 https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.
ENISA, ENISA Threat Landscape 2022: November 2022 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.
[107] https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach
[108] https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html
[109] https://www.reuters.com/article/global-cyber-solarwinds/hackers-at-center-of-sprawling-spy-campaign-turned-solarwinds-dominance-against-it-idUSKBN28P2N8
[110] Ledger is a provider of hardware wallet technology for cryptocurrencies.
[111] Ledger, 'Message by LEDGER's CEO – Update on the July data breach. Despite the leak, your crypto assets are safe'. https://www.ledger.com/message-ledgers-ceo-data-leak
[112] Inside The Scam: Victims Of Ledger Hack Are Receiving Fake Hardware Wallets, Nasdaq. https://www.nasdaq.com/articles/inside-the-scam%3Avictims-of-ledger-hack-are-receiving-fake-hardware-wallets-2021-06-17
[113] Mimecast is a supplier of cloud-based cybersecurity services, such as email security services, which require customers to connect securely to Mimecast servers to use their Microsoft 365 accounts.
[114] https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html
[116] Mellor, C., 'Kaseya VSA vulnerability opens a thousand-plus business doors to ransomware' , Blocks and Files, 2021 https://blocksandfiles.com/2021/07/04/kaseya-vsa-vulnerability-opens-1000-plus-business-doors-to-let-in-ransomware/

		Administrator (VSA) appliances of Kaseya's customers([115].	
Viasat	February 2022	Following the outbreak of the Russian war of aggression against Ukraine in February 2022, a denial of service attack on Viasat's KA-SAT network resulted in interruptions in consumer satellite broadband service [117].	The internet outage affected nearly 9 000 Nordnet subscribers, which is Viasat's client in France [118]. The attack had a spillover impact on an additional 40 000 Eutelsat subscribers, which relied on Viasat's KA-SAT satellite network. Outages were experienced in Germany, Greece, France, Italy, Hungary and Poland and lasted for several days [119]. Viasat reported that directly managed mobility or government users were not impacted.
Node Package Manager repository	March 2022	A threat actor dubbed 'RED-LILI' was linked to a large-scale supply chain attack campaign targeting the Node Package Manager repository.	Nearly 800 malicious modules were published [120].

[115] Kaseya is a software service provider specialising in remote IT monitoring and management tools, such as the VSA software. MSPs can use the VSA software onsite or they can license Kaseya's VSA cloud servers.
[117] https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview
[118] https://www.thejournal.ie/internet-cyber-attack-5701881-Mar2022/
[119] https://www.wionews.com/world/cyber-armageddon-in-europe-thousands-go-offline-following-russia-ukraine-war-says-report-459113
[120] https://blog.reversinglabs.com/blog/iconburst-npm-software-supply-chain-attack-grabs-data-from-apps-websites
https://www.bleepingcomputer.com/news/security/new-linux-macos-malware-hidden-in-fake-browserify-npm-package/
https://www.cisa.gov/news-events/alerts/2021/10/22/malware-discovered-popular-npm-package-ua-parser-js

ANNEX B: STANDARDS AND GOOD PRACTICES

This is a list of standards and good practices which are relevant to supply chain cybersecurity (in alphabetical order).

Cloud Security Alliance's Cloud Control Matrix (CCM) is a widely accepted framework with requirements for cloud service providers. Amongst others, it includes controls relevant to supply chain cybersecurity.

IEC 62443-2-4 defines requirements for a secure integrator process.

IEC 62443-3-3 defines technical requirements applicable for a system that can consequently be linked to product requirements.

IEC 62443-4-1 defines requirements for a secure development process and life cycle support.

IEC 62443-4-2 defines technical requirements applicable for products and components.

ISO 28000 addresses supply chains in general without addressing cybersecurity.

ISO 9001 defines requirements for a quality management system.

ISO/IEC 20243 describes security techniques and practices that could be used to mitigate risks on maliciously tainted and counterfeit products.

ISO/IEC 27001 defines an information security management system that also requires the addressing of supplier risks and supplier relationship with a comprehensive set of controls. Guidance on implementation of these controls are provided in ISO/IEC 27002. Further domain specific guidance on the ISO/IEC 27002 controls for telecommunication, cloud and energy is provided in ISO/IEC 27011, ISO/IEC 27017, and ISO/IEC 27019 respectively.

ISO/IEC 27036-series structures the supply chain security along the processes with supplier relationship planning, supplier selection, supplier relationship agreement, supplier relationship management and supplier relationship termination.

NERC CIP-013 defines for the electricity subsector a set of supply chain cybersecurity requirements and controls that includes notification and disclosure of vulnerabilities, incident requirements for vendors and verification of software integrity and patches.

NIST 800-161 defines a multitier risk management approach building on requirements defined in NIST SP 800-53.

US National Institute of Standards and Technology (NIST) Cybersecurity Framework for improving critical infrastructure cybersecurity includes controls for supply chain risk management.

NIST.SP.800-161r1: Supply Chain Risk Management, NIST

NISTIR 7622 Notional Supply Chain Risk Management Practices for Federal Information Systems, NIST

NISTIR 8276 Key Practices in Cyber Supply Chain Risk Management: Observations from Industry, NIST

ANNEX C: TERMINOLOGY

Table 12: Terminology on supply chain security

DORA	
ICT/OT third-party risk	ICT/OT risk that may arise for a financial entity in relation to its use of ICT/OT services provided by ICT/OT third-party service providers or by further subcontractors of the latter
ICT/OT third-party service provider	An undertaking providing digital and data services, including providers of cloud computing services, software, data analytics services and data centres, but excluding providers of hardware components and undertakings authorised under EU law which provide electronic communication services as defined in point (4) of Article 2 of Directive (EU) 2018/1972 of the European Parliament and of the Council.
Network Code for cybersecurity aspects of cross-border electricity flows	
Managed security service provider or MSSP	Any entity which provides outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services. MSSPs also include the use of high-availability security operation centres (either from their own facilities or from other data centre providers) to provide 24/7 services designed to reduce the number of operational security personnel an enterprise needs to hire, train and retain to maintain an acceptable security posture.
NIST.SP.800-161r1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organisations	
Acquirer	Organisation or entity that acquires or procures a product or service.
Cybersecurity risks throughout the supply chain	The potential for harm or compromise arising from suppliers, their supply chains, their products or their services. Cybersecurity risks throughout the supply chain arise from threats that exploit vulnerabilities or exposures within products and services traversing the supply chain as well as threats exploiting vulnerabilities or exposures within the supply chain itself.
Supplier	Organisation or individual that enters into an agreement with the acquirer or integrator for the supply of a product or service. This includes all suppliers in the supply chain, developers or manufacturers of systems, system components, or system services; systems integrators; suppliers; product resellers; and third-party partners.
Supply chain	Linked set of resources and processes between and among multiple levels of organisations, each of which is an acquirer, that begins with the sourcing of products and services and extends through their life cycle.

MITRE.org	
Supplier	Risks related to characteristics of a supplier of products or services, including their supply chain, that may potentially impact consumers of those products or services.
Supplies	Risks related to characteristics of supplies (products), including their supply chain provenance and pedigree, that may potentially impact consumers of those products.
Services	Risks related to characteristics of services, including their supply chain provenance and pedigree, that may potentially impact consumers of those services.
CISA.gov Alert (AA22-131A) Protecting Against Cyber Threats to Managed Service Providers and their Customers	
Managed Service Providers (MSPs)	Entities that deliver, operate or manage ICT/OT services and functions for their customers via a contractual arrangement, such as a service level agreement. In addition to offering their own services, an MSP may offer services in conjunction with those of other providers.
	Deliver services, such as network, application, infrastructure and security, via ongoing and regular support and active administration on customers' premises, in their MSP's data centre (hosting), or in a third-party data centre.
NISTIR 7622	
Acquirer	Stakeholder that acquires or procures a product or service.
Critical Component	A system element that, if compromised, damaged or failed, could cause a mission or business failure.
ICT/OT Supply Chain	Linked set of resources and processes between acquirers, integrators, and suppliers that begins with the design of ICT/OT products and services and extends through development, sourcing, manufacturing, handling, and delivery of ICT/OT products and services to the acquirer. NB: An ICT/OT supply chain can include vendors, manufacturing facilities, logistics providers, distribution centres, distributors, wholesalers, and other organisations involved in the design and development, manufacturing, processing, handling, and delivery of the products, or service providers involved in the operation, management and delivery of the services
ICT/OT Supply Chain Risk	Risks that arise from the loss of confidentiality, integrity or availability of information or information systems and reflect the potential adverse impacts to organisational operations (including mission, functions, image or reputation), organisational assets, individuals, other organisations and the state.
ICT/OT Supply Chain Risk Management	The process of identifying, assessing and mitigating the risks associated with the global and distributed nature of ICT/OT product and service supply chains

Supplier	Organisation or individual that enters into an agreement with the acquirer or integrator for the supply of a product or service. This includes all suppliers in the supply chain.
Digital Supply Chains Under Threat – Swedish Civil Contingencies Agency	
Digital supply chain	The services and infrastructures that deliver or enable the delivery of a digital product used to establish, maintain, develop or restore an organisation's information management and information systems.
ENISA Threat Landscape for Supply Chain Attacks	
Supplier	An entity that supplies a product or service to another entity.
Supplier Assets	Valuable elements used by the supplier to produce the product or service.
Customer	The entity that consumes the product or service produced by the supplier.
Customer Assets	Valuable elements owned by the target.

TP-03-23-145-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) is the EU's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost the resilience of the EU's infrastructure and, ultimately, to keep Europe's society and people digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-636-1
doi:10.2824/805268