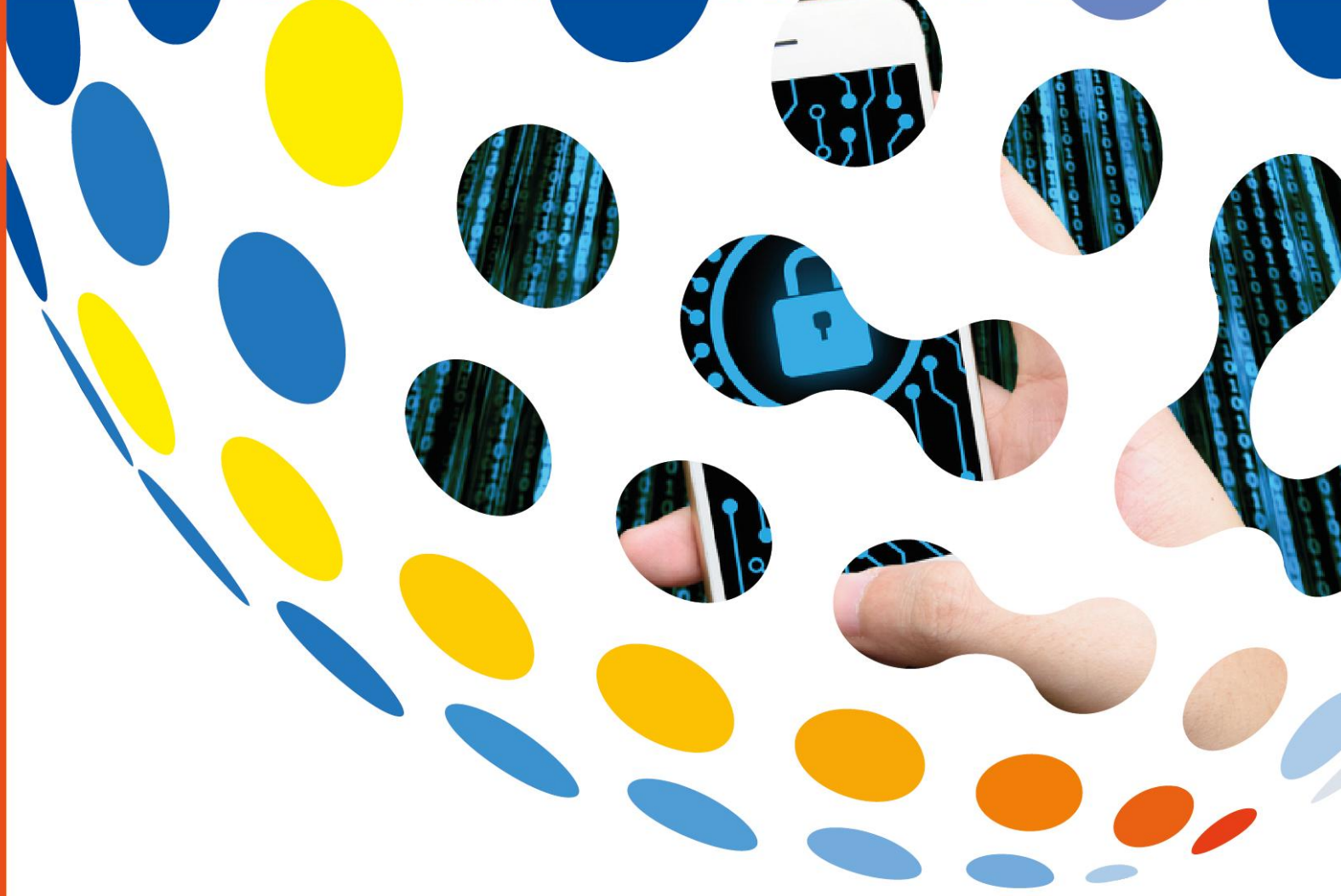

# EU ICT Supply Chain Security Toolbox

30 January 2026

NIS COOPERATION GROUP

# Executive summary

The EU Information and Communication Technology (ICT) Supply Chain Security Toolbox (hereafter 'ICT Supply Chain Security Toolbox') is the result of a collaborative effort by EU Member States, the European Commission and ENISA, as members of the NIS Cooperation Group Work Stream on Risk Assessment and Supply Chain Security. This document defines key concepts related to the ICT supply chain, identifies potential risk scenarios affecting ICT supply chains within the Union, and provides recommendations to address and mitigate these risks.

The ICT Supply Chain Security Toolbox provides Member States with a common, structured non-binding approach to securing their ICT supply chains. It also provides a general framework for Union level coordinated security risk assessments of critical supply chains based on Art. 22 of the NIS 2 Directive.

The recommendations and measures in the ICT Supply Chain Security Toolbox are primarily aimed at the Member States and cover the following areas:

| Recommendations |
|---|
| **Robust framework for ICT supply chain risk management** |
| R01. Establish and carry out ICT supply chain risk assessments |
| R02. Ensure a structured approach to ICT supply chain risk management |
| **Flexible, diverse and resilient ICT supply chains** |
| R03. Promote multi-vendor strategies and policies to address strategic dependency risks |
| R04. Manage and, if necessary, restrict or exclude high-risk suppliers at national level |
| **Situational awareness and operational cooperation** |
| R05. Promote information exchange, awareness, and training |
| **A resilient, trusted and transparent industrial base** |
| R06. Develop and support an interoperable ecosystem for secure supply chains |
| R07. Promote interoperability through the development and adoption of appropriate standards and certification |

## Disclaimer

The document is legally of non-binding nature. It is only of advisory character and therefore cannot alter the application of cybersecurity measures applicable in Member States. References to terms such as ‘critical supplier’ or ‘high-risk supplier’ should be understood as working concepts for the purpose of creating a common framework. Those are without prejudice to national laws implementing the NIS 2 Directive or sector-specific EU legislation, such as the Digital Operational Resilience Act (DORA).

This document can help Member States developing their approach to ICT supply chain security, as part of their national cybersecurity strategy according to Art. 7(2)(a) and assist them in the supervision of the requirements of Art. 21(2)(d) NIS 2 Directive.

The ICT Supply Chain Security Toolbox can also be useful to other public and private actors in assessing and mitigating supply chain risks of specific critical ICT services, ICT systems or ICT products.

# Table of Contents

**Executive Summary** ..... **3**

**1. Introduction** ..... **6**

1.1 Objectives ..... 8

1.2 Scope ..... 9

1.3 Development of the ICT Supply Chain Security Toolbox ..... 10

1.4 Legal framework and policy measures ..... 10

**2. Key concepts of the ICT Supply Chain Security Toolbox** ..... **15**

2.1 ICT supply chain and Supply chain entities ..... 15

2.2 Phases of the life cycle of ICT services, ICT systems and ICT products ..... 17

2.3 Supply chain incident ..... 18

2.4 Threats ..... 18

2.5 Vulnerabilities ..... 21

2.6 Impact ..... 22

**3. Risk scenarios** ..... **24**

3.1 Taxonomy for categorising risk scenarios ..... 25

3.2 Tailoring the risk scenarios ..... 25

3.3 Deliberate threats to ICT supply chains (malicious actions) ..... 27

Risk Scenario 1: Ransomware attack to a managed (security) service provider ..... 27

Risk Scenario 2: Geopolitical tensions with effects on a supplier in a third country, including legal implications ..... 28

Risk Scenario 3: Attack on a cloud computing provider ..... 29

Risk Scenario 4: Unauthorized insertion of counterfeit parts of a product via supplier to a trusted supplier ..... 30

3.4 Unintended threats to ICT supply chains (system failures and human errors) ..... 31

Risk Scenario 5: System failure within a government agency hosting network services to other public organisations ..... 31

Risk Scenario 6: Simultaneous ICT component failures at hospitals ..... 31

Risk Scenario 7: Data centre outage due to human error or malicious action prevents access to millions of websites and domains ..... 33

Risk Scenario 8: Faulty software update or vulnerability in a widespread system dependency ..... 34

3.5 Threats to ICT supply chains caused by external events or natural phenomena ..... 35

Risk Scenario 9: Supplier lock-in ..... 35

Risk Scenario 10: Natural disaster or pandemic causing a supply chain disruption ..... 36

Risk Scenario 11: ICT products and services cost volatility and supply chain disruptions…….. ....37
**4. Recommendations ....39**
4.1 Robust framework for ICT supply chain risk management ....40
R01: Establish and carry out ICT supply chain risk assessments ....40
R02: Ensure a structured approach to ICT supply chain risk management ....42
4.2 Flexible, diverse, and resilient ICT supply chains....43
R03: Promote multi-vendor strategies and policies to address strategic dependency risks ....43
R04: Manage and if necessary, restrict or exclude high-risk suppliers at national level ....45
4.3 Situational awareness and operational cooperation ....47
R05: Promote information exchange, awareness, and training....47
4.4 A resilient, trusted, and transparent industrial base ....48
R06: Develop and support an interoperable ecosystem for secure supply chains...48
R07: Promote interoperability through the development and adoption of appropriate standards and certification ....49
**5. Conclusions and review of the implementation....51**
Annex 1: Examples of threats relevant to ICT supply chains....53
Annex 2: Examples of vulnerabilities relevant to ICT supply chains ....57
Annex 3: Examples of impacts relevant to ICT supply chains ....61
Annex 4: Lifecycle phases ....64
Annex 5: Information sharing: Traffic Light Protocol ....67

# 1. Introduction

The protection of information and communication technology (ICT) supply chains is paramount for the Union's security, as they can play a crucial role in sustaining societal stability and driving economic activity across the Union. These supply chains enable the manufacture, production, distribution, and maintenance of ICT services, ICT systems and ICT products that underpin various critical sectors and sectors of high criticality, including healthcare, finance, transportation, telecommunication, and energy.

Certain components within ICT supply chains are critical due to their indispensable nature and potential impact on national security, public safety, and economic stability. These critical supplies encompass a range of materials, components, and technologies, including semiconductors, software, network infrastructure, and cybersecurity solutions.

Recognising the critical nature of ICT supply chains and essential supplies underscores the importance of safeguarding these systems against disruptions, vulnerabilities, and dependencies. Effective safeguards involve managing risks, enhancing resilience, diversifying sourcing strategies, fostering innovation, as well as promoting collaboration among stakeholders to manage vulnerabilities while ensuring the reliability, security, and continuity of ICT supply chains.

At Union level, the NIS 2 Directive provides for coordinated security risk assessments of critical ICT supply chains.[1] The coordinated security risk assessments of critical ICT supply chains should take into account both technical and, where relevant, non-technical factors.[2] The protection of ICT supply chains is also vital for small and medium-sized enterprises (SME), which are increasingly becoming the target of supply chain attacks due to their less rigorous cybersecurity risk-management measures and attack management, and the fact that they have limited security resources.[3]

[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.
[2] NIS 2 Directive, Recital (91).
[3] NIS 2 Directive, Recital (56).

On 9 March 2022, the informal meeting of the Telecommunications Ministers in Nevers resulted in a joint call, the so-called 'Nevers Call', to reinforce the EU's cybersecurity capabilities. It recognised that the "critical infrastructure such as telecommunications networks and digital services are of utmost importance to many critical functions in our societies and are therefore a prime target for cyberattacks". The call presented eight action items, including supply chain, focused on the enhancement of resilience of communications networks, the need to strengthen the market via public-private collaboration, the rapid adoption of the NIS 2 Directive and the need to build an ecosystem of trusted cybersecurity service providers.

Moreover, on 17 October 2022, the Council issued its Conclusions on ICT supply chain security[4], stating that it is of the "utmost importance to appropriately take the geopolitical environment into consideration not only when reacting to malicious cyber activities, but also when building and maintaining the resilience of information and communication technologies (ICT)". The Council highlighted the necessity of an all-hazard approach necessary to secure ICT assets. Strengthening the overall resilience and security of ICT supply chains is considered to be equally important as "enhancing resilience against supply chain attacks conducted via cyber means".

Additionally, the Council supports the "need to maximise and streamline the use of existing EU instruments […] as well as the need to continually adapt to the changing cyber threat landscape by introducing additional suitable measures and mechanisms". The Council invited the NIS Cooperation Group, in cooperation with the Commission and ENISA, to develop "a toolbox of measures for reducing critical ICT supply chain risks". Finally, the European Internal Security Strategy (ProtectEU) states that a harmonised approach to the security of the ICT supply chain can address the current fragmentation of the internal market caused by different approaches at national level, avoid critical dependencies and de-risk ICT supply chains from high-risk suppliers, in this way securing the critical infrastructure.[5]

[4] Council of the European Union, Council conclusions on ICT supply chain security, 17 October 2022, no. 13664/22. https://data.consilium.europa.eu/doc/document/ST-13664-2022-INIT/en/pdf

[5] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy, COM(2025) 148 final, 1 April 2025

To support the implementation of the NIS 2 Directive and in the spirit of the Council Conclusions, the NIS Cooperation Group, in cooperation with the Commission and ENISA, developed the present ICT Supply Chain Security Toolbox.

## 1.1 Objectives

The ICT Supply Chain Security Toolbox seeks to provide Member States with a common, structured non-binding approach to securing their ICT supply chains. The ICT Supply Chain Security Toolbox supports Member States by identifying selected risks associated with their ICT supply chains, and providing recommendations on how to strengthen the cybersecurity and resilience of their ICT supply chains. It also provides a general framework for preparing and conducting Union level coordinated security risk assessments of critical supply chains based on Art. 22 of the NIS 2 Directive.

The objectives of the ICT Supply Chain Security Toolbox can be summarised as follows:

- Create and foster a common understanding of ICT supply chain security risks;
- Identify potential threats, vulnerabilities, and risks within the ICT supply chain through a scenario-based methodology;
- Provide recommendations to secure the ICT supply chain.

The ultimate objective of the ICT Supply Chain Security Toolbox is to provide guidance on effective measures for managing security risks at each stage of the ICT services, ICT systems and ICT products lifecycle.

## 1.2 Scope

For the purpose of the ICT Supply Chain Security Toolbox, the subject matter of the risk assessments are ICT services, ICT systems or ICT products supply chains, encompassing hardware, software including free and open-source software (FOSS), and managed (security) services. The ICT Supply Chain Security Toolbox takes an all-hazards approach and considers technical and, where relevant, non-technical risk factors.

When evaluating suppliers, the NIS Cooperation Group recognizes the importance and the challenges for Member States to assess suppliers throughout the supply chain.

ICT supply chain risks need to be mitigated throughout the entire lifecycle of ICT services, ICT systems or ICT products.[6] Consequently, this ICT Supply Chain Security Toolbox defines the key phases of the lifecycle and identifies possible threats in each phase.

Importantly, the ICT Supply Chain Security Toolbox remains technology agnostic, focusing on the broader assessment of supply chain risks rather than targeting specific technologies. However, it provides risk scenarios and mitigation measures that are essential considerations when evaluating individual technologies.

The Member States play a key role in assessing the risks identified in this ICT Supply Chain Security Toolbox. To support Member States, the ICT Supply Chain Security Toolbox provides guidance in the form of risk scenarios and makes recommendations how to best address them, without assessing the scenarios or prioritising the measures. Furthermore, the European Commission has developed an "EU Methodology for Union level Cybersecurity risk assessments" designed to harmonise language and procedures, ensuring a coherent, cross-sectoral approach to Union level risk assessments.

[6] In detail see Annex 4.

## 1.3 Development of the ICT Supply Chain Security Toolbox

The steps taken when developing the ICT Supply Chain Security Toolbox:

1. Identification of supply chain phases and mapping with the subjects in scope, namely hardware, software, including FOSS and managed (security) services;
2. Identification of potential threats, based on an all-hazards approach;
3. Identification of potential threat actors;
4. Identification of potential vulnerabilities, if applicable;
5. Description of risk scenarios based on the identified threats, actors and vulnerabilities and, if applicable, for each phase/subject combination;
6. Recommendation of a set of mitigating measures addressed to Member States.

## 1.4 Legal framework and policy measures

The ICT Supply Chain Security Toolbox builds on an existing legal framework and complements policy measures already in place. The following non-exhaustive list provides an overview of these measures that contribute to strengthen the ICT supply chains security.

The **NIS 2 Directive**[7] lays the foundation for Union level security risk assessments of critical supply chains. Article 22(1) of the NIS 2 Directive provides that the NIS Cooperation Group, in cooperation with the European Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, ICT systems or ICT products supply chains, taking into account technical and, where relevant, non-technical risk factors. The European Commission, after consulting the NIS Cooperation Group and ENISA, and, where necessary, relevant stakeholders, shall identify specific critical ICT services, ICT systems or ICT products that may be subject to such Union level coordinated security risk assessment.

Pursuant to Article 21 of the NIS 2 Directive, Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and

[7] 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)

organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services. These measures have to be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and have to include supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers. Pursuant to Article 21(3) of the NIS 2 Directive, Member States have to ensure that, when considering which supply chain security measures referred to in Article 21(2), point (d), are appropriate, entities 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 considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1) of the NIS 2 Directive.

The **Commission Implementing Regulation (EU) 2024/2690**[8] lays down rules for the application of the NIS 2 Directive and specifies the technical and methodological requirements of cybersecurity risk-management in the sector of digital infrastructure.

The **Cyber Resilience Act (CRA)**[9] entered into force on 10 December 2024 and covers a wide range of hardware and software products, from microchips to routers and switches. The CRA will play a key role in securing ICT supply chains by:

- Requiring manufacturers of hardware and software products placed on the EU market, including their remote data processing solutions, to ensure that such

[8] Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

[9] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

products are developed in line with security-by-default and security-by-design principles, and that their security is maintained during a support period for the time the product is expected to be in use;

- Requiring a limited category of products explicitly listed in the CRA as class II important products or critical products to go through a third-party conformity assessment before their placement on the market;
- Facilitating supply chain security management for critical infrastructure covered by the NIS 2 Directive, including operators of public electronic communications networks and core Internet infrastructure;
- Requiring manufacturers to carry out risk assessments aiming to minimise cybersecurity risks, prevent security incidents and minimise the impacts of such incidents;
- Establishing new reporting obligations in case of severe incidents and actively exploited vulnerabilities contained in products with digital elements;
- Providing a light-touch regulatory regime on the FOSS and the so-called open-source software stewards.

Supply chain risks related to 5G networks, especially in relation to high-risk suppliers have already been identified and analysed in detail by Member States, with the support of the European Commission and ENISA, in the **EU coordinated risk assessment on 5G** published in October 2019.[10] To mitigate these risks, the **5G Toolbox**[11] recommends a set of strategic and technical measures, as well as corresponding supporting actions to reinforce their effectiveness.

[10] NIS Cooperation Group, EU-wide coordinated risk assessment of 5G networks security, 9 October 2019. https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

[11] NIS Cooperation Group, Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, 29 January 2020. https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

To complement the work on 5G cybersecurity, Member States carried out, together with the European Commission and ENISA, an in-depth **risk assessment of the EU's connectivity infrastructure sector**[12], which also identified threats and risks associated with suppliers (e.g., supply chain attacks or nation State interference on a supplier). This work led to a number of recommendations to increase the cybersecurity and resilience of these critical infrastructures. The findings of this work remain valid and relevant for the purpose of the ICT Supply Chain Security Toolbox.

The **Cybersecurity Act (CSA)**[13], which entered into force in 2019, plays a key role in shaping and enhancing the security of ICT supply chains by establishing a European cybersecurity certification framework, which aims to standardize and certify the security of ICT products, ICT services, ICT processes and managed security services in the Union. This certification framework promotes trust and transparency among stakeholders, facilitates cross-border trade, and enables informed decision-making by consumers and businesses when procuring ICT solutions. With Regulation (EU) 2025/37, the CSA was amended to enable the future adoption of European certification schemes for managed security services.

On 17 October 2022, the Council issued its **Conclusions on ICT supply chain security**[14], stating the "need to maximise and streamline the use of existing EU instruments […] as well as the need to continually adapt to the changing cyber threat landscape by introducing additional suitable measures and mechanisms". The Council invited the NIS Cooperation Group, in cooperation with the Commission and ENISA, to develop "a toolbox of measures for reducing critical ICT supply chain risks".

[12] NIS Cooperation Group, Report on the cybersecurity and resiliency of the EU communications infrastructures and networks, 21 February 2024. https://digital-strategy.ec.europa.eu/en/library/report-cybersecurity-and-resiliency-eu-communications-infrastructures-and-networks

[13] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification.

[14] Council of the European Union, Council conclusions on ICT supply chain security, 17 October 2022, no. 13664/22. https://data.consilium.europa.eu/doc/document/ST-13664-2022-INIT/en/pdf

The **EU Artificial Intelligence Act (AI Act)**[15] is a comprehensive legal framework for artificial intelligence, which entered into force on 1 August 2024. The AI Act introduces a uniform framework across all Member States, based on a forward-looking definition of artificial intelligence and a risk-based approach. It addresses potential risks to citizens' health, safety, and fundamental rights. The AI Act provides developers and deployers with clear requirements and obligations regarding specific uses of artificial intelligence.

[15] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence

# 2. Key concepts of the ICT Supply Chain Security Toolbox

This section presents the following key concepts of the ICT Supply Chain Security Toolbox:

- ICT supply chain and Supply chain entities,
- Phases of the life cycle of ICT services, ICT systems or ICT products,
- Supply chain incident,
- Threats and vulnerabilities within ICT supply chains,
- Potential impacts of supply chain incidents.

These concepts provide the basis for the risk scenarios in Chapter 3. Examples and further details of the concepts can be found in Annex 1, 2, 3, and 4.

## 2.1 ICT supply chain and Supply chain entities

The ICT supply chain refers to the network of entities/organisations, people, processes, logistics, technology, and resources engaged in activities and creating value from the sourcing of materials through the delivery of ICT services, ICT systems or ICT products[16]. This may include the supply of systems, hardware, software, information or communication services (typically cloud computing services, managed services, and others) as well as potential risks that arise deeper within the ICT supply chain (e.g. microchip manufacturers, open-source libraries, or third-country subcontractors).

The supply chain includes different type of entities, all contributing to the final delivery to the user:

**Supplier** is a legal or natural person that provides products or services to individuals or organisations, including public administration and businesses. Suppliers play a critical role in the supply chain by ensuring the availability, functionality, and security of various solutions. Suppliers are categorized into different types based on the nature

[16] Adapted definition from ISO 22300:2021(en) Security and resilience - Vocabulary.

of the products and services they provide, and they include ICT suppliers, as defined below.

**ICT supplier** is a legal or natural person that offers ICT services, ICT systems or ICT products to individuals or organisations, like public administration or businesses.[17] ICT suppliers play a crucial role in the ICT technological ecosystem by offering a range of solutions, including hardware, software, networking equipment, and services while facilitating the distribution and support of ICT services, ICT systems or ICT products.

**Critical supplier** is a legal or natural person that supplies ICT services, ICT systems or ICT products whose disruption, compromise or modification could seriously affect the public security and safety of entities or citizens, or the functioning of the internal market of the EU, for example by affecting an essential service or causing strong, widespread and simultaneous disruptions across the society or within a specific sector (spillover effect). A supplier may be considered critical for several reasons: For example, if a supplier is the source of a monodependency[18], meaning that multiple organisations rely on its ICT services, ICT systems, or ICT products without any alternatives to fall back on. Another reason a supplier may be deemed critical is if their ICT services, ICT systems, or ICT products are essential to the operation of a particularly important service. For instance, a cloud service provider with a small client base could still be critical if one of its clients is an emergency service relying on it to store critical data.

**Manufacturer** means a natural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed or manufactured, and markets them under its name or trademark, whether for payment, monetisation or free of charge.[19] As such, their due diligence is crucial in preventing vulnerabilities from moving up the supply chain.

[17] Other terms commonly used for supplier are vendor, contractor, producer, retailer, or seller.
[18] An organisation has a dependency on, for instance, a service if it 1) uses that service, 2) needs to use that service, and 3) has no available alternative services to use if that one service becomes unavailable. A monodependency exists when multiple organisations, either within a specific sector or across society, have a dependency on the same service.
[19] CRA, Article 3(13).

**Managed Service Provider (MSP)** provides 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.[20]

**Managed Security Service Provider (MSSP)** means a MSP that carries out or provides assistance for activities relating to cybersecurity risk management.[21]

**Cloud Computing Provider** offers a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations.[22]

**User** is any legal or natural person, or group of persons utilising ICT services, ICT systems or ICT products.[23] User includes an end user in the supply chain.

## 2.2 Phases of the life cycle of ICT services, ICT systems and ICT products

Supply chains include every step that is involved in getting a finished product or service to the customer or end user. In the context of ICT supply chains, it is crucial to distinguish the individual steps/phases of the whole life cycle of ICT services, ICT systems and ICT products.

The phases considered for the ICT Supply Chain Security Toolbox are:

1. **Design**, including requirements specification and architecture;
2. **Development and production**, including raw material procurement and testing/quality assurance;
3. **Distribution**, including logistics and transportation;
4. **Acquisition**, including retail/sales;
5. **Deployment**, including installation/configuration;
6. **Maintenance**, including use and support/updates; and
7. **Disposal/decommissioning/archiving**.

[20] NIS 2 Directive, Article 6(39).
[21] NIS 2 Directive, Article 6(40).
[22] NIS 2 Directive, Article 6(30).
[23] Alternatively, customer, consumer or acquirer.

## 2.3 Supply chain incident

ICT supply chains play a critical role in enabling the global digital infrastructure and underpin the functioning of modern societies and economies. As a result, incidents within these ICT supply chains can pose significant threats to the Union. An incident means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems.[24] Such an event may affect the availability, authenticity, integrity or confidentiality of an ICT product. In line with this, a supply chain incident refers to an incident (as defined above), in which something that:

a) **Should be delivered** (e.g. a new software feature or antivirus signature in an update) **is not delivered**, or

b) **Should not be delivered** (e.g. malware concealed in a software update or a limiting configuration in a component) **is delivered**.

## 2.4 Threats

As threats to the security of network and information systems can have different origins, the all-hazard approach provides guidance for the ICT Supply Chain Security Toolbox categorisation and identification of threats. To ensure alignment between previous work on the underlying causes of incidents and the all-hazard approach, the threats identified to ICT supply chains are sorted according to the root cause categories proposed by the NIS Cooperation Group.[25] Further details can be found in Annex 1.

| |
|---|
| **Malicious action** |
| **System failure** |
| **Human error** |
| **Natural phenomena/external event** |

[24] NIS 2 Directive, Art. 6(6).
[25] NIS 2 Directive, Recital (79). Specific examples within these categories are in Annex 1.

### 2.4.1 Threat actors

The ICT Supply Chain Security Toolbox focuses on more skilled threat actors since these are the actors who can do the most harm. Malicious activity targeting supply chains can be in form of sophisticated digital activity or can also be linked to the physical access to a targeted component. Consequently, highly motivated and skilled actors are treated with priority as the most probable ones.

As traditional targeted entities respond to the threat landscape by raising their cyber resilience, malicious actors have a particular incentive to attack a vulnerable ICT supply chain, given that a successful supply chain attack may result in a desired objective. The desired objective may be financial gains, such es extortion or non-financial gains such as severely impacting the security of network and information systems used by governments, societies and private organisations, disrupting critical infrastructures and compromising or gaining access to sensitive data. For the same reason, a supply chain attack may be deemed the most effective approach by aiming at multiple or specific targets, all or many of which can be affected simultaneously through a single ICT supply chain entity.

The following threat actors are more likely to have the skills and capability required to target the ICT supply chain:[26]

| Actor | Description |
|---|---|
| State-nexus threat groups | Often referred to as Advanced Persistent Threats (APTs), they are in general well-funded, resourced and display advanced capabilities. Their primary objectives typically include, espionage, revenue generation and conducting disruptive attacks to further promote the strategic objectives of their nation state. Such objectives may be pursued by the military, intelligence or state control apparatus of their country. State-nexus groups do not only target other governments. They can also target other organisations for sensitive data or conduct operations to obtain funding for their country. |
| Organised crime groups | They are motivated predominantly by financial gain. Their attacks tend to be opportunistic and indiscriminate. They target the data or infrastructure that has the highest impact on the operations of victims. Cybercrime actors have shown an increased level of collaboration and professionalisation. |

[26] Based on the ENISA Threat Landscape 2023, October 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

| | |
|---|---|
| Hackers-for-hire | They are actors that contribute to the professionalisation of the cybercrime market and they also provide services to state-nexus groups. There is a black market of attack tools, where organised crime groups offer advanced tools and services to attackers with limited technical skills. |
| Hacktivist groups | They are not as well-resourced as the other threat actors but are often fuelled by strong – mainly ideological – motivations. Their objectives often involve disruption, and they use hacking to affect some form of political or social change. |
| Insiders | They are within an otherwise trusted organisation, may work for an organised crime group, a hacktivist group or a state actor, or have other individual motivations. |

Several competent authorities have observed an increasing overlap between different types of threat actors. For example, state-nexus threat groups are making greater use of malware and services provided by organised crime groups. Ransomware attacks have also been employed for sabotage purposes or as a cover to conceal espionage operations.

### 2.4.2 High risk suppliers

In the context of ICT supply chain, high-risk suppliers can represent a significant threat actor to supply chains and are included in the relevant risk scenarios. The 5G Toolbox recommends assessing the risk profile of suppliers based on several factors, which are also relevant for this ICT Supply Chain Security Toolbox, such as the likelihood of the supplier being subject to interference from a third country; the supplier's ability to assure supply; the overall quality of products and cybersecurity practices of the supplier.[27]

[27] More specifically, the 5G Toolbox recommends looking at:

- The likelihood of the supplier being subject to interference from a non-EU country. Such interference may be facilitated by, but not limited to, the presence of the following factors:
  - A strong link between the supplier and a government of a given third country;
  - the third country's legislation, especially where there are no legislative or democratic checks and balances in place, or in the absence of security or data protection agreements between the EU and the given third country;
  - The characteristics of the supplier's corporate ownership;
  - The ability for the third country to exercise any form of pressure, including in relation to the place of manufacturing of the equipment.
- The supplier's ability to assure supply.
- The overall quality of products and cybersecurity practices of the supplier, including the degree of control over its own supply chain and whether adequate prioritisation is given to security practices.

| Actor | Description |
|---|---|
| High risk supplier | They are likely to be subject to interference from a third country, which can be linked to jurisdiction applicable to the manufacturer, the characteristics of its corporate ownership and the links of control to a third-country government where it is established.[28]<br><br>High-risk suppliers are those whose involvement may significantly increase the likelihood or impact of supply chain compromise, disruption, or espionage. A supplier may be deemed high risk based on factors such as:<br>• Jurisdictional exposure to countries with no legislative or democratic checks and balances in place or frequent government interference.<br>• Supplier corporate ownership subject to interference from a third country.<br>• Poor security or quality performance, including known cybersecurity or product integrity issues.<br>• Supply assurance risks due to political, legal, or trade instability.<br>• Lack of transparency or unwillingness to cooperate with audits or regulations. |

## 2.5 Vulnerabilities

Vulnerabilities are defined as a weakness, susceptibility or flaw of ICT products, ICT systems or ICT services that can be exploited by a cyber threat.[29] They can be understood as a lack of something that may either prevent, or help prevent an incident, for example, missing critical software patches or gaps in organisational cybersecurity practises.

The ICT Supply Chain Security Toolbox considers both ICT vulnerabilities and other supply chain related vulnerabilities, e.g., dependence on service or related supplier performance, or the high complexity of software and hardware technology products and the extent to which supply chains are interconnected. Moreover, vulnerabilities in an ICT supply chain are related to the characteristics of the specific technology or the

The assessment of a supplier's risk profile may also take into account notices issued by EU authorities and/or Member States national authorities.

The Commission applied these criteria in the Communication from the Commission on the implementation of the 5G cybersecurity Toolbox of 15 June 2023.

[28] A supplier may also be considered high-risk due to its geographical location, for instance if the area is vulnerable to natural disasters or geopolitical events.

[29] NIS 2 Directive, Article 6(15). For products, CRA, Article 3(40) applies.

sector that may be assessed. Examples of vulnerabilities in the ICT supply chain are given in Annex 2.

The general categories of vulnerabilities[30], which may apply to ICT services, ICT systems or ICT products, are:

| ICT vulnerabilities |
| --- |
| **Physical infrastructure vulnerabilities** |
| **Poor cybersecurity practices by the supplier** |
| **Poor supply chain practices by the user** |
| **Supply chain dependency vulnerabilities** |
| **Economic vulnerability** |
| **Supplier vulnerability specific to the legal jurisdiction of a third country** |

## 2.6 Impact

Potential impacts of a supply chain incident can range from impacts on the user or the supplier, to impacts on societal, national or even international level. Potential consequences may relate to health, functioning of society, economy, safety and security and democratic values. The impact and consequences of an incident may under certain circumstances spill-over to a broader range of users or sectors than anticipated or foreseen. In the context of supply chain security, the spill-over effect refers to the potential impact or consequence that cyber incidents in one part of the supply chain can have on other interconnected parts. It denotes that supply chain security risks have the potential to spread beyond their point of origin and affect different phases or actors within the supply chain network. The spill-over effect highlights the linked and interdependent nature of modern supply chains, where an exploited vulnerability or threat event in one area can spread and have cascading effects. For instance, low-level or widely used components may pose wider cross-

[30] Specific examples within these categories are in Annex 2.

sectoral risks due to their widespread use. Examples of impacts relevant to ICT supply chains are given in Annex 3.

A list of potential impacts comprises the following:

| |
|---|
| **Data leakage, loss or tampering (confidentiality, integrity)** |
| **Financial impact or loss** |
| **Reputational damage** |
| **Impact on service quality, integrity or disruption (availability, integrity)** |
| **Legal repercussions** |
| **Geopolitical and strategic national impacts** |
| **Impact on public safety** |
| **Political impact** |

# 3. Risk scenarios

This section describes eleven main risk scenarios that are of strategic importance at the Union level, depending on the level of risk identified by the Member States. The risk scenarios are indicative, high-level scenarios that can be used for risk assessments in several sectors. Since the ICT Supply Chain Security Toolbox takes an all-hazards approach, the risk scenarios reflect the fact that incidents can arise from a wide range of causes. This approach seeks to assess various risks and analyses the potential sources of those risks, aiming to protect network and information systems as well as their physical environments. To manage cybersecurity risk effectively, it is essential to address also the physical and environmental security of network and information systems, ensuring they are protected from different types of threats.

Risk scenarios have been identified in the following documents:

- ENISA threat landscape for supply chain attacks[31];
- EU-wide coordinated risk assessment of 5G networks security[32];
- Report on the cybersecurity and resiliency of the EU communications infrastructures and networks[33];
- EU cybersecurity risk evaluation and scenarios for the telecommunications and electricity sectors[34];
- Member States' risk assessments and security perspectives;
- CISA's Supplier, Products, and Services Threat Evaluation (version 3.0)[35].

[31] ENISA Threat Landscape for Supply Chain Attacks, 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

[32] NIS Cooperation Group report, EU coordinated risk assessment of the cybersecurity of 5G networks, 9 October 2019. https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

[33] NIS Cooperation Group, Cybersecurity and resiliency of Europe's communications infrastructures and networks, 21 February 2024. https://digital-strategy.ec.europa.eu/en/library/report-cybersecurity-and-resiliency-eu-communications-infrastructures-and-networks

[34] NIS Cooperation Group, EU cybersecurity risk evaluation and scenarios for the telecommunications and electricity sectors Follow up to the Council Conclusions on the EU's Cyber Posture of 23 May 2022 and Council Conclusions on the EU Policy on Cyber Defence of 22 May 2023, 24 July 2024. https://digital-strategy.ec.europa.eu/en/news/risk-assessment-report-cyber-resilience-eus-telecommunications-and-electricity-sectors

[35] Cybersecurity and Infrastructure Security Agency (CISA), Information and Communications Technology Supply Chain Risk Management Task Force, Threat Evaluation Working Group: Supplier, Products, and Services Threat Evaluation, Version 3.0, 2021. https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v3.pdf

## 3.1 Taxonomy for categorising risk scenarios

Building on the definition of a supply chain incident and the four main categories of threats – malicious actions, system failure, human error and natural phenomena/external events) – outlined in Chapter 2, the following taxonomy was developed to categorise the eleven risk scenarios (RS):

| | **Compromise of availability, authenticity, integrity and confidentiality** | |
|---|---|---|
| | Something that should be delivered is not delivered | Something that should not be delivered is delivered |
| **Malicious action** | RS1, RS2 | RS3, RS4 |
| **System failure** | RS5 | RS6 |
| **Human error** | RS7 | RS8 |
| **Natural phenomena/ external event** | RS9, RS10, RS11 | --[36] |

This taxonomy is used to emphasise the multiple threats that can result in incidents within the ICT supply chain. Many of the incidents described in the following risk scenarios could stem from different types of threats.

## 3.2 Tailoring the risk scenarios

The eleven scenarios described in this ICT Supply Chain Security Toolbox are indicative and adopt an all-hazard approach. Rather than focusing on a single threat category, the wide range of risks that can impact ICT supply chains is reflected. This taxonomy is intended to illustrate the diversity of potential threats and provide concrete scenarios that can be modified to different contexts, for example when being used for

[36] No plausible incidents were identified falling into the category of delivery of something that should not be delivered as a consequence of natural phenomena or external events.

specific supply chain risk assessments. Examples of such variations may include the following:

- Scenarios of malicious action (RS1, RS2, RS3, RS4) can be tailored to include other types of malicious actions, e.g. alternative external cyber-attack, or deliberate internal action instead of an external cyber-attack.
- Scenarios of system failures or human errors (RS5, RS6, RS7, RS8) can be modified to describe scenarios where the root cause is a malicious action. For instance, RS7 addresses the human factor affected by lack of awareness, but it could also be caused by an intentional, malicious action (e.g. sabotage). Similarly, RS8 addresses human error, but it could also be caused by system failures (potentially linked to poor cybersecurity practices).
- Scenarios may also be modified to combine threat sources. This could include, for example, an operational error that is not indicating a new dependency (undocumented usage of software). After a vulnerable update is released, a malicious actor might exploit an unpatched vulnerability in the undisclosed dependency.
- Scenarios of natural phenomena or external events (RS9, RS10, RS11) can be adjusted to reflect other types of external events, such as financial risks at the supplier side, labour issues, environmental risks or political instability.
- Scenarios can be adjusted to include different entities within the supply chain that may be impacted (e.g. the various types of entities which contribute to the final delivery to the user, as described in Section 2.1). For instance, RS1 could be extended to cover subcontractors or suppliers with administrative access to an organisation's ICT systems.

It is important to note that malicious actions often take place within complex threat landscapes, where the lines between state-nexus threat groups and organised crime groups are becoming increasingly blurred.

In the next sections the eleven risk scenarios are described. For each scenario a narrative description explains how the scenario unfolds and the main consequences are outlined. Each scenario is accompanied by a table that provides a structured

overview of key elements of the scenario, according to the concepts explained in Section 2 and Annexes 1 to 4.

| | |
|---|---|
| **Type of supply chain incident** | See Section 2.3 |
| **Threat causing the incident** | See Section 2.4, detailed description in Annex 1 |
| **Involved supply chain entities** | See Section 2.1 |
| **Phases involved** | See Section 2.2, detailed description in Annex 4 |
| **Threat actor** | See Section 2.4.1 and 2.4.2 |
| **Vulnerability** | See Section 2.4, detailed description in Annex 2 |
| **Impact** | See Section 2.5, detailed description in Annex 3 |

## 3.3 Deliberate threats to ICT supply chains (malicious actions)

### Risk Scenario 1: Ransomware attack to a managed (security) service provider

Company X provides IT services to thousands of public and private organisations in various sectors. The company provides managed services that form the core of operations for many of its customers, which are found in several EU countries.

A criminal group exploits an unpatched vulnerability in one of Company X's on-premises servers to gain access to infrastructure that is essential to the operation of the organisation. The group then launches a ransomware attack on the servers hosting many of the company's customers' websites and applications. To put even more pressure on Company X, the group threatens to launch a DDoS attack against the company's infrastructure and leak data that was allegedly collected during the attack.

During the weeks it takes for the company to restore its services, many of Company X's customers experience operational disruptions. Many of the organisations directly affected by the incident are heavily dependent on Company X's services and have no alternative solutions, leaving them unable to resume to normal operations for several days or weeks. As Company X provides IT services in several countries within the Union, citizens and organisations in many EU countries are affected.

Due to the number of organisations affected and the possible cascading effects that the incident may have triggered, the extent of the incident is difficult to grasp. Consequently, joint efforts of several EU countries are required. Following the incident, Company X and some of its customers suffer reputational damage. As many

customers perceive Company X's security measures as inadequate, legal proceedings are initiated against the company, which leads to a continuous loss of its customer base.

| | |
|---|---|
| **Type of supply chain incident** | Something that should be delivered is not delivered |
| **Threat causing the incident** | Malicious action |
| **Involved supply chain entities** | Managed service provider, User |
| **Phases involved** | Maintenance |
| **Threat actor** | Organised crime groups |
| **Vulnerability** | ICT vulnerabilities, Poor cybersecurity practices by the supplier, Poor supply chain security practices by the user |
| **Impact** | Data leakage, loss or tampering (confidentiality, integrity), Financial impact or loss, Reputational damage, Impact on service quality or disruption (availability, integrity), Legal repercussions |

### Risk Scenario 2: Geopolitical tensions with effects on a supplier in a third country, including legal implications

Company A, a major ICT supplier from Country Y, provides critical telecommunications equipment and software to many countries, including Country X, a Member State. Company A has been a stable supplier of goods essential for Country X's critical infrastructure for many years. However, as the political situation in Country Y changes, the relations between Country X and Y are deteriorating. New laws in Country Y require domestic companies to prioritise national security over international contracts, allowing government intervention and retroactive alteration of contracts. Intelligence reports also indicate ties between Country Y's government and Company A.

Companies in Country X suddenly face challenges enforcing contractual terms with Company A, who cite national laws to avoid compliance with data security and transparency requirements. For example, Company A has failed to implement security updates and provide audit reports, citing national security regulations. Company A also moved sensitive data to their jurisdiction, against the agreement.

The situation for Country X is complicated by the fact that there is only a limited number of suppliers capable of delivering equivalent products, making it challenging for companies in Country X to find alternative suppliers. As geopolitical tensions increase, Country Y escalates the situation by imposing restrictions. As a result, Country X can

no longer access goods supplied by Country Y, which hinders necessary repairs and maintenance of critical infrastructure.

| | |
|---|---|
| **Type of supply chain incident** | Something that should be delivered is not delivered |
| **Threat causing the incident** | Malicious action[37] |
| **Involved supply chain entities** | ICT supplier, User |
| **Phases involved** | Maintenance, design, development |
| **Threat actor** | High-risk supplier |
| **Vulnerability** | ICT vulnerabilities, Poor cybersecurity practices by the supplier, Supplier vulnerabilities specific to the legal jurisdiction of a third country[38], Supply chain dependency vulnerabilities |
| **Impact** | Impact on service quality or disruption (availability, integrity), Geopolitical and strategic national impacts, Data leakage, loss or tampering (confidentiality, integrity) |

### Risk Scenario 3: Attack on a cloud computing provider

A major cloud computing provider (Company X) hosts critical infrastructure for numerous organisations worldwide, including the EU. It offers services such as virtual machines, storage, and databases. Its reputation for security and reliability is crucial to its business. A sophisticated malicious cyber actor infiltrates a third-party software supplier that provides Company X with a critical management tool. The supplier's update server is compromised, allowing the attackers to inject malicious code into the next software update. Company X unknowingly installs the tainted update, which includes a backdoor and provides persistent access to its infrastructure.

As a subsequence, the malicious cyber actor identifies valuable customer data (e.g., user credentials, payment information, intellectual property), exfiltrates the data to an external server and maintains access for future attacks. While having access to the infrastructure, the malicious actor may also sabotage the third-party software.

| | |
|---|---|
| **Type of supply chain incident** | Something that should not be delivered is delivered[39] |
| **Threat causing the incident** | Malicious action |
| **Involved supply chain entities** | ICT supplier, Cloud Computing Provider, User |

[37] See Annex 1, where a geopolitical threat is also malicious in nature.
[38] See Annex 2, where supplier vulnerabilities specific to the legal jurisdiction of a third country are explained.
[39] The identified type of supply chain incident refers to the attack on the supplier of the critical management tool.

| | |
|---|---|
| **Phases involved** | Distribution, Deployment, Maintenance |
| **Threat actor** | State-nexus threat groups or Organised crime groups |
| **Vulnerability** | ICT vulnerabilities, Poor cybersecurity practices by the supplier |
| **Impact** | Data leakage, loss or tampering (confidentiality, integrity), Financial impact or loss, Legal repercussions |

### Risk Scenario 4: Unauthorized insertion of counterfeit parts of a product via supplier to a trusted supplier

A third party (Supplier X) supplying components (software or hardware) to a reputable supplier (Supplier Y) within the supply chain does not undergo the same rigorous vetting process as the trusted supplier. A threat actor gains access to Supplier X's systems, infiltrating the network, gaining control over critical infrastructure, such as inventory databases, production line management, and shipping processes. The malicious cyber actor introduces counterfeit parts into Supplier X's inventory. The attackers manipulate records or tampers with inspection procedures. The counterfeit parts pass-through Supplier X's checks and are deemed suitable for distribution. Supplier X ships the counterfeit parts to a vetted supplier (e.g., an automobile manufacturer). Based on the trust levels already established between the suppliers, Supplier Y simply integrates these parts directly into their assembly line without performing typical due diligence checks. The counterfeit parts are then used in the production of end products (e.g., cars). The threat actor can collect user data, such as the location of the vehicle or can cause intentional system failures and jeopardise the safety of specific individuals.

| | |
|---|---|
| **Type of supply chain incident** | Something that should not be delivered is delivered |
| **Threat causing the incident** | Malicious action |
| **Involved supply chain entities** | ICT supplier, Manufacturer, User |
| **Phases involved** | Design, Development & Manufacture, Distribution, Acquisition & Deployment, Maintenance |
| **Threat actor** | State-nexus threat groups, Organised crime groups or Insiders |
| **Vulnerability** | Poor cybersecurity practices by the supplier, Poor supply chain practices by the user |
| **Impact** | Data leakage, loss or tampering (confidentiality, integrity), Impact on service quality or disruption (availability, integrity), Geopolitical and strategic national impacts, Impact on public safety |

## 3.4 Unintended threats to ICT supply chains (system failures and human errors)

### Risk Scenario 5: System failure within a government agency hosting network services to other public organisations

A large number of public organisations in sectors such as healthcare, transportation, and emergency services, are dependent on the network infrastructure provided by government agency X for their daily operations. Government agency X's physical infrastructure, which supports the functioning of the network, is significantly outdated. Despite reports warning about the risks posed by the aging equipment, upgrades and replacements have been delayed due to budget constraints and competing priorities within the agency. A hardware failure at one of government agency X's primary data centres results in an interruption in the network. This in turn, affects the services provided by the many public organisations that are dependent on the network. Until the affected hardware is replaced, hospitals cannot access critical systems, public transportation face coordination issues, and citizens cannot reach emergency services.

| | |
|---|---|
| **Type of supply chain incident** | Something that should be delivered is not delivered |
| **Threat causing the incident** | System failure |
| **Involved supply chain entities** | ICT supplier, User |
| **Phases involved** | Maintenance |
| **Threat actor** | State-nexus threat groups, Organised crime groups or Insiders |
| **Vulnerability** | ICT vulnerabilities, Poor cybersecurity practices by the supplier |
| **Impact** | Impact on service quality or disruption (availability, integrity), Impact on public safety |

### Risk Scenario 6: Simultaneous ICT component failures at hospitals

Several hospitals in Country X rely on computers supplied by Company X for critical operations such as patient records, diagnostics and administrative functions. Over the course of a few weeks, about a thousand computers from Company X experience failures of ICT components, namely hard drives. With so many computers failing at the same time, some hospitals must resort to manual processes, which significantly slows down their operations.

Due to an inadequate service level agreement between the hospitals and Company X, the cause of the incident takes a long time to diagnose. It is later discovered that the hardware damage to the computers is due to a misconfiguration that causes them to fail after a certain number of operating hours. The misconfiguration also makes the computers vulnerable to attacks, which underlines the urgency of replacing the affected computers.

Despite that the cause of the incident is identified, replacement and repairs continue to be delayed due to the large volume of failures and limited availability of replacement components. In the meantime, hospitals must operate under significant constraints, reducing their capacity and increasing the risk of medical errors occurring, due to a reliance on manual processes. The lack of contingency plans worsens the impact of the incident in some hospitals. After the incident, Country X cancels its contract with Company X.

| | |
|---|---|
| **Type of supply chain incident** | Something that should not be delivered is delivered |
| **Threat causing the incident** | System failure |
| **Involved supply chain entities** | ICT supplier, User |
| **Phases involved** | Development and production, Maintenance |
| **Threat actor** | State-nexus threat groups, Organised crime groups or Insiders |
| **Vulnerability** | ICT vulnerabilities, Poor cybersecurity practices by the supplier, Poor supply chain practices by the user, Supply Chain Dependency Vulnerabilities |
| **Impact** | Financial impact or loss, Impact on service quality or disruption (availability, integrity), Impact on public safety |

### Risk Scenario 7: Data centre outage due to human error prevents access to millions of websites and domains

A major cloud service provider experiences a severe outage when one of its primary data centres overheats, leading to the sudden unavailability of servers responsible for hosting millions of websites, including critical government and public authority domains across multiple countries. The outage affects approximately 2% of all Country X's domains, leaving essential services offline and inaccessible to the public.

The disruption is traced to human error, where personnel, who were relatively new and unfamiliar with established protocols, mistakenly closed vital air vents when leaving the data centre. This oversight caused the facility to overheat rapidly, leading to widespread service interruptions. Despite the cloud service provider's swift response to reroute traffic through alternative data centres, a large portion of the primary service capacity from the affected data centre remains offline for several days.

As a result, millions of users, including those depending on essential government services, face significant delays and disruptions. The extended downtime raises concerns about personnel training, adherence to protocols, and the overall resilience of the cloud service provider's infrastructure.

| | |
|---|---|
| **Type of supply chain incident** | Something that should be delivered is not delivered |
| **Threat causing the incident** | Human error |
| **Involved supply chain entities** | Cloud computing provider, User |
| **Phases involved** | Maintenance |
| **Threat actor** | State-nexus threat groups, Organised crime groups or Insiders |
| **Vulnerability** | Poor cybersecurity practices by the supplier, Poor supply chain practices by the user |
| **Impact** | Reputational damage, Impact on service quality or disruption (availability, integrity) |

### Risk Scenario 8: Faulty software update causing widespread system failures

Company X relies on a critical software application developed by a well-established third-party supplier (Supplier X), who is responsible for maintaining and enhancing the software throughout its life cycle. Supplier X, among other services, provides regular antivirus updates on the critical software applications of a large EU multinational corporation to protect its data and information. The purpose of the antivirus software is to detect and address new malware in the application and needs a continuous supply of new “signatures” that allow it to handle the constant stream of new malware.

The antivirus software program, which Supplier X uses, requires a high level of access permissions in the application but also other information systems at Company X, right down to the core functions of the operating system. Supplier X ensures that this is necessary in order to protect against malware in all levels of the software.

This makes trust in the antivirus software provider critical to the Company X. To maintain rapid response capabilities against emerging threats, Supplier X push updates to its clients quickly. Since Company X relies on the speed of these updates, they are rarely subjected to detailed checks and are instead uploaded automatically through a trust-based network.

However, due to human error and insufficient testing procedures, Supplier X releases a faulty software update that contains a coding error. As the software update is uploaded automatically, the faulty update goes unnoticed and causes Company X’s information systems to go offline. Since thousands of companies in the EU are dependent on Supplier X’s software update, a large number of information systems go down at the same time. As these systems become unavailable, it triggers cascading failures across the region, leading to widespread system failures in critical systems across the EU. Supplier X suffers reputational damage as the adequacy of its testing procedures is questioned.

| | |
|---|---|
| **Type of supply chain incident** | Something that should not be delivered is delivered |
| **Threat causing the incident** | Human error |
| **Involved supply chain entities** | ICT supplier, Managed Security Service Provider, User |
| **Phases involved** | Design, Distribution, Deployment, Maintenance |

| | |
|---|---|
| **Vulnerability** | Poor cybersecurity practices by the supplier, Poor supply chain practices by the user |
| **Impact** | Reputational damage, Impact on service quality or disruption (availability, integrity) |

## 3.5 Threats to ICT supply chains caused by external events or natural phenomena

### Risk Scenario 9: Supplier lock-in

Company X, a multinational financial service provider, invests and strengthens its cybersecurity due to increasing threats and regulations. Company X choses Company Y and Company Z for a three-year contract to deploy firewalls, intrusion detection systems, and endpoint protection software. There are just a few specialized companies with the knowledge required to perform the required work. As Company X expanded, it integrated more of Company Y's and Z's products and services.

Over time, Company X's reliance on Company Y and Z grew, with custom scripts and automation built around their application programming interfaces (APIs). At some point, Company Z went suddenly bankrupt, and given the deep integration of software systems and the lack of additional providers with such a specific knowledge, the replacement of Company Z was taken over by Company Y to avoid serious disruptions and a lengthy and uncertain replacement of Company Z. Despite rising costs, Company X continued investing in Company Y's ecosystem due to its performance and reliability. This also resulted in more companies choosing Company Y services, increasing their influence, market shares and customers.

By the third year, Company X faced challenges with delayed support, slower response times, and escalating service costs. Company Y announced significant price increases, exploiting their dominant position. Licensing costs rose, and Company X faced penalties for non-compliance. Company X discouraged interoperability with other suppliers, making it difficult to introduce new technologies.

Company X found itself locked into Company Y's ecosystem, with expensive migration solutions, application rewrites, staff retraining, and potential service disruptions preventing any serious migration attempts.

| | |
|---|---|
| **Type of supply chain incident** | Something that should be delivered is not delivered |
| **Threat causing the incident** | External event |
| **Involved supply chain entities** | ICT supplier, Managed Security Service Provider, User |
| **Phases involved** | Design, Development and production, Deployment, Maintenance |
| **Vulnerability** | Supply chain dependency vulnerabilities, Poor supply chain practices by the user, Economic vulnerability |
| **Impact** | Financial impact or loss |

### Risk Scenario 10: Natural disaster or pandemic causing a supply chain disruption

A massive earthquake strikes Country X, damaging key tech manufacturing hubs and semiconductor plants. Critical infrastructures like transportation and power grids are destroyed, halting production of microchips, circuit boards, and memory modules.

After two weeks, the factories have to be closed, leading to shortages of ICT components. Companies scramble for alternative suppliers, but face challenges due to the lack of suppliers for these highly specialised components. As many ICT companies are reliant on the damaged facilities in Country X, they are forced to scale-down their own operations. Thus, many of them suffers financial consequences.

The shortage of critical components is further intensified by insufficient buffer stocks. While some companies had prepared for supply chain disruptions, inventories were quickly depleted, forcing them to compete for limited stocks. Consequently, prices for existing components skyrocket, which worsens the crisis.

| | |
|---|---|
| **Type of supply chain incident** | Something that should be delivered is not delivered |
| **Threat causing the incident** | Natural phenomena |
| **Involved supply chain entities** | ICT supplier, Manufacturer, User |
| **Phases involved** | Development and production, Distribution, Acquisition, Deployment, Maintenance |
| **Vulnerability** | Supply chain dependency vulnerabilities, Poor supply chain practices by the user, Physical infrastructure vulnerabilities |
| **Impact** | Financial impact or loss, Impact on service quality or disruption (availability, integrity) |

### Risk Scenario 11: ICT products and services cost volatility and supply chain disruptions

The global ICT sector is profit driven, making it fragile to input cost fluctuations and critical to broader economic and national security stability. Whereas moderate price changes may be absorbed in other industries, the ICT sector is more vulnerable to economic volatility, particularly where it concerns essential components and services.

Amid macroeconomic instability and shifting geopolitics, policy measures increasingly disrupt the movement of high-tech goods, critical raw materials, and digital services. Export restrictions, constraints on specialised manufacturing capacities, shifts in foreign investment, tax and monetary changes, and diverging regulations drive up costs for semiconductors, rare earths, specialised metals and server-grade batteries, while limiting the availability of cross-border cloud and data services.

This leads to a surge in ICT goods and service prices, compounding supply disruptions. The disruption spreads rapidly across ICT-dependent sectors. Enterprises in areas including telecommunications, health tech, and AI services encounter severe delays in procuring critical hardware and software. Rising costs make it unsustainable to maintain ICT infrastructure, leading to service degradation and operational failures. New data centre projects are suspended or cancelled, and AI developers struggle to comply with legal requirements due to the inaccessibility of requisite protective technologies and support services within the internal market at viable cost.

Organisations are compelled to seek alternative suppliers, renegotiate contracts, or suspend critical innovation programmes. SMEs are particularly exposed due to limited financial and operational resilience. From a technological perspective, for example edge network devices are particularly at risk.[40] In response, governments promote strategic digital autonomy through reshoring, local production, and increased oversight of supply chain dependencies.

[40] Edge network devices encompass appliances, such as firewalls, routers, virtual private networks (VPN) gateways, Internet of Things (IoT) devices, internet-facing servers, and internet-facing operational technology (OT) systems. Guidance and strategies to protect edge network devices can be found here: CISA, Security considerations for edge devices (ITSM.80.101) and Canadian Centre for Cyber Security Mitigation strategies for edge devices: Executive guidance (cyber.gov.au)

In the short term, these interventions can lead to further fragmentation of the global ICT landscape and to uncertainty in procurement, interoperability, and service continuity. However, it should be noted that in the long term such interventions can contribute to the supply chain resilience, thus reducing cost volatility.

| | |
|---|---|
| **Type of supply chain incident** | Something that should be delivered is not delivered |
| **Threat causing the incident** | External event (financial risks, political instability) |
| **Involved supply chain entities** | Manufacturers (ICT component manufacturers, contract hardware assemblers), Cloud computing providers, ICT suppliers (software developers, logistics providers), User (public and private sector) |
| **Phases involved** | Design, Development and Production, Distribution, Acquisition, Deployment and Maintenance |
| **Vulnerability** | Economic vulnerability, Supply chain dependency vulnerabilities, Supplier vulnerabilities specific to the legal jurisdiction of a third country |
| **Impact** | Financial impact or loss, Impact on service quality or disruption (availability, integrity) |

# 4. Recommendations

The identified potential risk scenarios underline the need to promote secure ICT supply chains. To achieve this objective in due time, a clear set of measures is recommended. This section provides a description of these measures, highlighting their significance, implementation steps, and expected outcomes to promote secure ICT supply chains and improve cybersecurity while following a risk-based approach and ensuring proportionality. It is important to acknowledge that some of the recommendations will take time to achieve and must be approached in several stages.

The NIS 2 Directive and the Commission Implementing Regulation (EU) 2024/2690, which specifies the technical and methodological requirements of cybersecurity risk-management in the sector of digital infrastructure, already include a set of technical, operational, and organisational measures to promote the cybersecurity of ICT supply chains.

Furthermore, the CRA sets out horizontal cybersecurity requirements for products with digital elements and is expected to add transparency and improve the security of supply chains. As part of the implementation of the CRA, Member States will need to increase their capabilities to respond to market needs, ensuring companies wishing to place products on the market have access to suitable infrastructure for testing and conformity assessment, as well as capabilities of market surveillance authorities to support market actors.

The supply chain risks related to 5G networks, in particular related to high-risk suppliers, are specifically addressed in the 5G Toolbox. Given the importance of the connectivity infrastructure for the digital economy and dependence of many critical services on 5G networks, the implementation of the 5G Toolbox is essential, yet it remains sectoral. To complement this sector-specific approach and to ensure broader coverage of supply chain risks, Member States should align their horizontal efforts with the implementation of the present ICT Supply Chain Security Toolbox.

To complement and further enhance these measures, the following recommendations for Member States, and EU institutions, bodies, offices and agencies have been identified.

| Recommendations |
| --- |
| **4.1 Robust framework for ICT supply chain risk management** |
| R01. Establish and carry out ICT supply chain risk assessments<br>R02. Ensure a structured approach to ICT supply chain risk management |
| **4.2 Flexible, diverse and resilient ICT supply chains** |
| R03. Promote multi-vendor strategies and policies to address strategic dependency risks<br>R04. Manage and, if necessary, restrict or exclude high-risk suppliers at national level |
| **4.3 Situational awareness and operational cooperation** |
| R05. Promote information exchange, awareness, and training |
| **4.4 A resilient, trusted and transparent industrial base** |
| R06. Develop and support an interoperable ecosystem for secure supply chains<br>R07. Promote interoperability through the development and adoption of appropriate standards and certification |

## 4.1 Robust framework for ICT supply chain risk management

### R01: Establish and carry out ICT supply chain risk assessments

Member States should take further steps in establishing and carrying out ICT supply chain risk assessments at national level and, when applicable, support Union level coordinated risk assessments pursuant to Art. 22 NIS 2 Directive by contributing knowledge in the specific area of a risk assessment. Member States should ensure that supply chain risks in the critical sectors, selected by the NIS Cooperation Group or at national level, are assessed in a timely manner and that critical suppliers for the Member States are identified. To the extent possible, potential disruptions and emerging threats should be anticipated.

- For Member States it is recommended to implement the following measures:
    - Define the scope of national risk assessments taking into account the supply chains or the sectors, which are considered a priority for the Member State. Where applicable, take into account the results of EU-coordinated risk assessments based on Art. 22 NIS 2 Directive.
    - Carry out national supply chain risk assessments on a regular basis taking into account relevant European and international standards, the ICT Supply Chain Security Toolbox risk scenarios and, where applicable,

the results from EU-coordinated risk assessments based on Art. 22 NIS 2 Directive.

- Consider using for national risk assessments the principles of the EU Methodology for Union-level Cybersecurity Risk Assessments.
- Support the process of identifying the topics for and the performance of Union level coordinated security risk assessments by the NIS Cooperation Group, in cooperation with the European Commission and ENISA.
- Ensure that relevant national authorities have the necessary empowerment and means in place to collect information from entities about suppliers and their provided products in critical sectors with clear data-sharing guidelines to avoid excessive administrative burden and to monitor such information on a regular basis.
- Define national and/or sectorial criteria in the form of a guidance for the relevant entities to assess the criticality of their suppliers. The results of this assessment should be communicated by the relevant entities to the national authorities.
- Identify critical suppliers[41] and assess supply chain risks. This can be achieved either by setting up a mechanism to identify relevant assets and carrying out assessment of the risks in that Member State pursuant to Article 7(1)(d) NIS 2 Directive, or by addressing cybersecurity in the supply chain for ICT products and ICT services used by entities for the provision of their services.
- At national level, analyse and map critical dependencies, including monodependencies, and identify potential sources of dependencies and single points of failure. To assess the risk of these dependencies, the dependencies of relevant entities on suppliers should be aggregated at the national level for both sectors and products, based on the reported information on suppliers of relevant entities in critical sectors.
- Take into account the specific risks to sensitive data (both public and private), including the possibility of illicit access to such data through ICT suppliers. When assessing the risk, consider both technical and non-

[41] See the definition of a 'critical supplier' in section 2.1.

technical risk factors, such as legislation that would allow access to data without consent.

- Relevant risk scenarios: RS1 to RS11

**R02: Ensure a structured approach to ICT supply chain risk management**

Member States should ensure that the entities follow a structured approach to supply chain risk management which complements the measures of the NIS 2 Directive and the CRA. The entities should be aware of their ICT supply chain risks (transparency), analyse, and mitigate those risks taking into account, where applicable, the state-of-the-art and relevant European and international standards.

- For Member States it is recommended to implement the following measures:
  - Support important and essential entities in taking appropriate and proportionate cybersecurity risk management measures (as defined under Article 21 of the NIS 2 Directive) to manage identified supply chain security risks and, where applicable, monitor their effectiveness and progress.
  - Provide adequate and publicly available guidance to entities, especially SMEs, on appropriate measures to manage supply chain security risks and methods for monitoring effectiveness of measures, to be developed by the NIS Cooperation Group.
  - Ensure that entities guarantee, for example through contractual arrangements and assurance mechanisms, that their critical suppliers implement appropriate, proportionate and measurable cybersecurity risk management measures to mitigate identified supply chain security risks; competent authorities may consider issuing binding instructions to the entity to remedy deficiencies. These measures should be based on Art. 21 NIS 2 Directive. This means ensuring that the critical suppliers consider regular security audits, vulnerability assessments, incident response planning, and adherence to recognised security standards. Additionally, where applicable, establish mechanisms for continuous monitoring and reporting to assess their effectiveness and track progress over time.

- Expanding upon the Commission's Implementing Regulation[42], to establish a directory of suppliers and service providers, consider applying this to other entities, originally not in scope.
- Consult the ENISA Technical Guidance for the Cybersecurity Measures of the NIS Implementing Act[43].
- Conduct preparedness tests or stress tests to ensure that the relevant entities have implemented the appropriate risk management measures and are resilient against threats to the supply chain with the objective to validate and not replace the entities own responsibility in performing regular stress tests.
- Based on the identified vulnerabilities and threats, consider monitoring and/or ensuring that products and services delivered or used by entities have been adequately tested on established testing platforms and/or sandbox environments.

- Relevant risk scenarios: RS1, RS3, RS4, RS5, RS6, RS7, RS8, RS10, RS11

## 4.2 Flexible, diverse, and resilient ICT supply chains

### R03: Promote multi-vendor strategies and policies to address strategic dependency risks

Member States should, where feasible, adopt policy and regulatory measures ensuring that entities have a multi-vendor strategy in place to secure critical ICT supply chains. This approach should seek to limit high dependency risks by avoiding reliance on single suppliers (monodependencies) and limit vendor lock-in, whenever possible. The goal is to promote policies that diversify critical ICT supply chains.[44]

- For Member States it is recommended to implement the following measures:

[42] Point 5 of Annex 1 of the Commission Implementing Regulation (EU) 2024/2690.
[43] ENISA Implementation guidance on Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures, October 2024, Draft for public consultation (not published, to be published in 2025).
[44] Supplier diversification refers to the strategic approach of engaging multiple suppliers to ensure the resilience, security, and continuity of ICT supply chains. It aims to reduce systemic risks associated with over-reliance on a single supplier, enhance competition, and foster a more robust and adaptive technological ecosystem.

- Develop and implement, where feasible, multi-vendor strategies and policies at the national level to address strategic dependency risks.
- Consider friendshoring/nearshoring[45] which can limit risks from both geopolitical threats and climate related incidents etc.
- Identify thresholds above which the entities identified by Member States as critical diversify suppliers of specific ICT services, ICT systems or ICT products. These thresholds should be based on objective criteria, national risk assessments, and in collaboration with the affected entities. For other entities, encourage them to diversify suppliers of specific ICT services, ICT systems or ICT products, above identified thresholds. Criteria for diversification thresholds could include, but are not limited to:
    - Supplier market share dependency: If a single supplier holds a dominant position for critical ICT services, ICT systems or ICT products.
    - Geopolitical risk exposure: If a significant portion of the supply chain is concentrated in/controlled by high-risk geopolitical regions.
    - Supplier cybersecurity compliance: If a supplier does not meet baseline cybersecurity standards.
    - Single point of failure risk: If supplier failure would cause major operational disruption (e.g., over 24 hours of downtime for critical services).
- Ensure supplier diversification, including through public procurement requirements as well as through financial and regulatory incentives for entities implementing multi-vendor strategies in accordance with EU and national legal frameworks.
- Ensure, where more than one suitable supplier exists, that entities in critical supply chains should:
    - Develop and implement multi-vendor strategies and policies to address high dependency risks.

[45] Friendshoring is a supply chain strategy where manufacturing and sourcing is done from countries that are considered trusted geopolitical allies. These may include the rerouting of supply chains to countries perceived as politically and economically safe or low-risk, to avoid disruption to the flow of business. Nearshoring is a strategy where a company shifts its supply chain or production to a nearby country, often sharing a border with the target country.

        - Consider diversification of their ICT supply chains across a wider range of locations, sources and assets and build resilience in these supply chains.
        - Work towards redundancy of suppliers by dual- or multi-sourcing supply as well as secure interoperability to foster a seamless operation between services.
    - Consider applying point 5.1.2 (d) of Annex I of the Commission Implementing Regulation (EU) 2024/2690 also to other entities, originally not covered by the scope of the Commission Implementing Regulation.
- Relevant risk scenarios: RS1, RS2, RS3, RS5, RS6, RS7, RS9, RS10, RS11

**R04: Manage and if necessary, restrict or exclude high-risk suppliers at national level**

Member States should assess the risk profile of critical suppliers in order to identify high-risk suppliers by following a common Union level approach with coordinated risk assessments based on Art. 22 NIS 2 Directive. Therefore, the assessment should be based on the collected information about suppliers, their mapping (see R01), and predefined criteria. Member States should also take into account existing EU coordinated risk assessments. Following this assessment, Member States take measures to manage high risk suppliers in accordance with national policies and regulations.

- For Member States it is recommended to implement the following measures:
    - Establish a national framework to evaluate critical suppliers[46] based on defined criteria in order to identify high-risk suppliers. Such criteria could include, but are not limited to:
        - The likelihood of the supplier being subject to interference from a third country. Such interference may be facilitated by, but not limited to, the presence of the following factors:
            - A strong link between the supplier and a government of a given third country.
            - The third country's legislation, especially where there are insufficient legislative or democratic checks and balances

[46] See the definition of a 'critical supplier' in section 2.1.

in place, or in the absence of security or data protection agreements between the EU and the given third country.[47]

- The characteristics of the supplier's corporate ownership.
- The ability for the third country to exercise pressure, including in relation to the place of manufacturing of the equipment.

- The supplier's ability to restrict or deny supply, or to deliver something unauthorized.
- The cybersecurity practices of the supplier, including the degree of control over its own supply chain and whether adequate prioritisation is given to cybersecurity practices.
- The assessment of a supplier's risk profile may also take into account notices issued by EU authorities and/or national authorities.
- The supplier is subject to a jurisdiction of a third country where, according to a public statement on behalf of the EU or its Member States, threat actors operating from the territory of that third country have carried out malicious cyber activities or campaigns.
- The supplier is subject to a jurisdiction of a third country that is collecting vulnerabilities to use in offensive attacks.

- Ensure that entities assess the risk profile of suppliers based on the defined criteria and guidelines to identify high-risk suppliers and dependencies on such suppliers (see above).
- Ensure national policies and/or regulations are in place in order to take decisions to restrict or exclude high-risk suppliers from supply chains identified as critical based on the national risk assessment, including, where available, the results of the EU coordinated risk assessments. In other parts of the supply chain (not identified as critical), take appropriate measures to minimise the risk posed by that supplier to the rest of the supply chain.

[47] In this context, several Member States attribute a higher risk profile to suppliers that are under the jurisdiction of third countries conducting an offensive cyber policy.

- Based on the results of the risk profile assessment of suppliers and potential restrictions/exclusions or other measures, include relevant cybersecurity-related requirements for ICT services, ICT systems or ICT products in procurement and adjust awarding criteria to ensure secure ICT supply chains and encourage private entities to do the same.

- Relevant risk scenarios: RS2, RS11

## 4.3 Situational awareness and operational cooperation

### R05: Promote information exchange, awareness, and training

Member States should aim for increased cooperation to exchange information and best practices about ICT supply chain security matters within the relevant cooperation platforms at the national and EU levels. ENISA should facilitate information sharing at EU level, provide guidance to Member States and industry, develop training programs, and promote awareness of supply chain cybersecurity, secure procurement and usage practices of ICT services, ICT systems or ICT products.

- For Member States it is recommended to implement the following measures:
  - Communicate the outcome of national risk assessments to the NIS Cooperation Group, applying confidentiality measures where necessary, and contribute to Union level risk assessments on this basis, if available.
  - Share progress and challenges on the implementation of the supply chain security measures in the context of the NIS Cooperation Group.
  - Develop and standardise the collection and analysis of incidents related to the ICT supply chain (including supply chain attacks) in the context of Article 29 of the NIS 2 Directive ('Cybersecurity information-sharing arrangements'). Where possible and without prejudice to competencies in national security, consider incorporating:
    - country-specific intelligence (e.g. national security threat assessments),
    - known incidents, along with cyber threat intelligence, and
    - where available, the results of the Union wide dependency assessment for specific categories of products with digital elements, according to Art 13(25) of the CRA.

- Share information on ICT supply chain incidents within the NIS Cooperation Group, the European cyber crisis liaison organisation network (EU-CyCLONe) and the CSIRTs network.[48]
- Support entities to build the right skills across their workforce to manage supply chain security. Examples: Cybersecurity Skills Academy Communications from the EC (2023/207 final) and Advanced Digital Skills co-funding supports from Digital Europe Regulation (2021/695).
- Promote awareness of supply chain cybersecurity nationally, in collaboration with ENISA (industry workshops, training, and knowledge-sharing initiatives on supply chain security).
- Exchange good practices on the implementation of the ICT Supply Chain Security Toolbox recommendations within the NIS Cooperation Group.
- Promote the use of the ICT Supply Chain Security Toolbox risk scenarios for cybersecurity exercises at national and international level.

- Relevant risk scenarios: RS1 to RS11

## 4.4 A resilient, trusted, and transparent industrial base

### R06: Develop and support an interoperable ecosystem for secure supply chains

Members States should promote the development of an ecosystem at EU level leveraging economic benefits together with increased security in the supply chain. Initiatives that aim to reduce strategic dependencies and to strengthen the ecosystem of European suppliers should be promoted nationally and at EU level.

- For Member States it is recommended to implement the following measures:
  - Foster EU-initiatives to develop the ecosystem of European suppliers and support EU industry to secure supply chains, and by closely cooperating with the ECCC.
  - Ensure that ICT projects supported with public funding reflect cybersecurity risks and the recommendations of the ICT Supply Chain Security Toolbox.

[48] The importance of cooperation and information sharing across sectors and communities is at the core as well of the recently adopted Council Recommendation on an EU-blueprint for cybersecurity crisis management, C/2025/3445, 20 June 2025, http://data.europa.eu/eli/C/2025/3445/oj

- Include cybersecurity-related requirements for ICT services, ICT systems or ICT products in public procurement, such as the diversification of suppliers, adjust awarding criteria to ensure secure supply chains and encourage entities to do the same.
- Ensure appropriate and suitable measures are in place to support SMEs in line with the CRA, such as through awareness-raising and support programmes targeting SME compliance and transformation needs.
- Promote the security and visibility of open-source software and hardware, particularly where this could help secure the supply chain of critical entities, and promote the adoption of secure open-source alternatives, for instance by
  - open-sourcing existing public sector solutions,
  - through the creation of open-source programme offices, and
  - diversifying digital internet infrastructures, such as code repositories or encryption certificate authorities.

- Relevant risk scenarios: RS2, RS4, RS5, RS9, RS10, RS11

**R07: Promote interoperability through the development and adoption of appropriate standards and certification**

Member States should promote the development and adoption of appropriate standards and certification schemes at EU level, building on existing European and international frameworks and in collaboration with European Standardization Organizations, and other relevant bodies. EU frameworks, standards, or European cybersecurity certification schemes should support interoperability, contributing to Union wide effects, market awareness and a level playing field. Where no relevant European cybersecurity certification scheme is yet applicable under the Cybersecurity Act (CSA), national certification schemes may also support interoperability.

This measure includes recommendations for entities for certifying ICT products, ICT services, and ICT processes under the CSA, supported by national policies for high-risk suppliers based on EU coordinated security risk assessments of critical supply chains pursuant to Article 22 of the NIS 2 Directive.

- For Member States it is recommended to implement the following measures:

- Ensure adequate representation of European interests in existing standardisation and certification fora, whether European or international.
- Ensure adequate participation in maintenance of certification schemes and standards, integrating relevant information on new vulnerabilities and ensuring it is adequately disseminated throughout the supply chain.
- Promote a coordinated assessment of vulnerabilities, bringing together resources from market surveillance, industry and security researchers and taking due account of the respective EU frameworks and the need for a coherent overview of the internal market.
- Promote open standards and secure-by-design principles to facilitate multi-supplier environments.

- Relevant risk scenarios: RS2, RS9, RS11

# 5. Conclusions and review of the implementation

The ICT Supply Chain Security Toolbox is designed to promote a common approach to ICT supply chain security, including policy and regulatory measures, supply chain risk management, analysis and mapping of high-risk suppliers, adherence to recognised standards, certification, and interoperability, information exchange, awareness, and training, development of the ecosystem of European suppliers.

| Recommendations | Risk scenarios | How this recommendation addresses mitigation measures |
|---|---|---|
| **Robust framework for ICT supply chain risk management** | | |
| **R01. Establish and carry out ICT supply chain risk assessments** | RS1 to RS11 | This recommendation addresses the systematic identification of supply chain assets, vulnerabilities and threats to ensure transparency as well efficacy when choosing mitigating measures. |
| **R02. Ensure a structured approach to ICT supply chain risk management** | RS1, RS3, RS4, RS5, RS6, RS7, RS8, RS10, RS11 | This recommendation addresses the selection of appropriate and proportionate cybersecurity risk management measures. |
| **Flexible, diverse, and resilient ICT supply chains** | | |
| **R03. Promote multi-vendor strategies and policies to address strategic dependency risks** | RS1, RS2, RS3, RS5, RS6, RS7, RS9, RS10, RS11 | This recommendation addresses management of (mono)dependencies |
| **R04. Manage and if necessary, restrict or exclude high-risk suppliers at national level** | RS2, RS11 | This recommendation addresses the issues involved in managing high-risk suppliers |
| **Situational awareness and operational cooperation** | | |
| **R05. Promote information exchange, awareness, and training** | RS01 to RS11 | This recommendation addresses the need to increase the general level of knowledge and training when dealing with ICT supply chain risks. |
| **A resilient, trusted and transparent industrial base** | | |
| **R06. Develop and support an interoperable ecosystem for secure supply chains** | RS2, RS4, RS5, RS9, RS10, RS11 | This recommendation addresses building an ecosystem focused on secure supply chains and interoperability. |
| **R07. Promote interoperability through appropriate standards and certification** | RS2, RS9, RS11 | This recommendation addresses the support needed in the development, adoption and promotion of standards and certifications. |

By implementing these recommendations, the EU and its Member States can enhance supply chain resilience and improve cybersecurity.

The NIS Cooperation Group should regularly review the implementation of the above-mentioned recommendations. Approximately one year after the adoption of the ICT Supply Chain Security Toolbox, the Work Stream will hold a “tour de table” to assess progress, identify challenges and best practices, and propose adjustments where necessary. To prepare for this discussion, the Task Force will circulate a survey to all NIS Cooperation Group members, collecting information on how Member States have implemented the recommended measures and the lessons learned gained from this process.

# Annexes

## Annex 1: Examples of threats relevant to ICT supply chains

The ICT Supply Chain Security Toolbox's categorisation of threats to the ICT supply chain is based on an all-hazards approach and is aligned with the previous NIS Cooperation work on Cybersecurity Incident Taxonomy[49]. The Cybersecurity Incident Taxonomy classifies the nature of an incident by the type of threat that triggered the incident, i.e. the root cause.

The list of threats below is based on the taxonomy by the NIS Cooperation.[50] A few examples are also provided where appropriate, to demonstrate the fit to the supply chain risk assessment.

**Malicious action**

- Deliberate internal action, e.g.
    - Tampering (introduction of weaknesses, backdoors)
    - Introduction of malware or unvetted code into software products
    - Data theft or espionage
    - Privileged access to user's system
    - Installation of counterfeit parts[51] (e.g. compromised components, counterfeit certificates of products or services)
- Deliberate physical damage/manipulation/theft/other deliberate action (e.g. terrorism, physical attacks, sabotage, compromise)
- External cyber-attack, e.g.
    - Malware infection (e.g., Remote Access Trojan (RAT), backdoor, ransomware, spyware)
    - Exploiting software vulnerability
    - Exploiting configuration vulnerability

[49] NIS Cooperation Group Publication 04/2018, Cybersecurity Incident Taxonomy, July 2018 https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53646

[50] The category "process failure" was included in "system failure". The category "third party failure" is not used as it is relevant for all risk scenarios in this toolbox.

[51] Replacement or substitution of trusted or qualified supplier components, products, or services with those from potentially untrusted sources.

    - Surveillance software by State actor
    - Data breaches
    - Social engineering attacks
    - DoS/DDoS – Resource depletion
- Geopolitical threats, e.g.
    - Nation State interference on a supplier
    - Imposed sanctions and regulations that can impact directly on suppliers and their access to components critical to product development
    - Dependency on suppliers in third countries and increased risk to coercion

**System failure**

- Hardware capacity and performance
    - Installation or use of faulty or compromised third-party hardware
- Hardware maintenance
    - Installation or use of faulty or compromised third-party hardware
- Hardware obsolescence/ageing
- Software compatibility/configuration
    - Installation or use of faulty or compromised third-party software
    - Introduction of malware or unvetted code into software products or production of a programme with non-standard or even intrusive features
    - Use of vulnerable open-source libraries
    - Compromise of developer and distribution systems of a software provider
    - Non-standard procedures concerning patching, including inability to patch or delay or purposeful omittance of discovered vulnerabilities due to various reasons (financial, technological, insufficient capacities and safety instruments, etc.)
    - Release of an infected or ineffective software update
    - Poor system development and design principles or practices (e.g. undocumented usage of third-party software)
- Software performance
    - Inadequate change management (e.g. reduced quality of service due to change of the provider)
- Network configuration

- Physical damage
- Process failure
    - Deficient monitoring and control (e.g. unavailability of ICT products, for instance, due to shortages of critical raw materials and semiconductors needed for their production)
    - Improper operations (e.g. disruption of production, logistical issues such as lost/damaged shipments, customs clearance delays)
    - Inadequacy of internal procedures and documentation (e.g. increasingly complex regulation resulting in e.g. longer lead times to complete customs clearance)
    - Recovery failures or redundancy issues
    - Innovation lag[52]

**Human error**

- Mistake or omission (e.g. human error resulting in physical disruption to supply route)
- Skills and knowledge (e.g. lack of training, poor cyber hygiene practices, poor cybersecurity awareness of staff)
- Inadequate human resources (e.g. inadequate vetting process, insufficient/unclear delineation of roles and responsibilities)
- Communication issues

**Natural Phenomena/External event**

- Natural disaster/force majeure, e.g. (non-exhaustive list):
    - Extreme weather events disrupting or impacting the supply chain (e.g. manufacturing and distribution channels and associated supply routes)
    - Epidemics and pandemics causing severe disruption to labour availability and physical access restrictions
- Environmental risk impacting on supply of raw materials required to produce products (e.g. pollutants, scarcity of raw materials)
- Labour issue (e.g. skills shortage, strikes)

[52] i.e., slow adoption of new technologies from a significant supplier of the supply chain could lead to bottlenecks, delays, and other disruptions.

- Political instability affecting supply chains, e.g. war
- Financial and economic risk (e.g. bankruptcy of supplier, trade sanctions imposed on supplier, global pricing and currency fluctuation, rising costs (e.g. energy, fuel, transportation, wages, raw materials, etc.))

# Annex 2: Examples of vulnerabilities relevant to ICT supply chains

### ICT vulnerabilities

- Software vulnerabilities, including vulnerable open-source libraries, delay in software updates and patches
- Network vulnerabilities
- Hardware vulnerabilities
- Vulnerable end-user device
- Misconfigurations
- Unsecured APIs
- Unsecure default configurations

### Physical infrastructure vulnerabilities

- Access control vulnerabilities
- Environmental vulnerabilities
- Structural vulnerabilities
- Perimeter security vulnerabilities

### Poor cybersecurity practices by the supplier

- Poor authentication practises, inadequate or improperly implemented access control to certain resources, data, or systems within an organisation
- Low cybersecurity awareness of staff
- Inadequate security solutions
- Inadequate practices and procedures for reviewing and assessing code during the development process
- Inadequate or insufficient practices for testing software, systems, and applications for vulnerabilities and flaws
- Insufficient systems and practices for observing and analysing network traffic, system activities, and user behaviours to identify irregularities that may indicate a security incident
- Lack of security measures for updates, e.g. code signing or integrity checks
- Lack of traceability of parts and poor-quality checks

- Security through obscurity due to the proprietary security solutions used by the supplier
- Absence of multi-factor authentication (MFA)
- Excessive privileges / lack of least-privilege enforcement
- Unclear incident response roles and escalation procedures
- No regular review of security events
- No regular security training or phishing simulations
- Lack of role-based security training for developers and admins
- No independent security testing (penetration tests, audits)

**Poor supply chain practices by the user**

- Insufficient systems and practices for observing and analysing network traffic, system activities, and user behaviours to identify irregularities that may indicate a security incident
- Weak supplier risk assessment
- Inadequate contractual requirements including cybersecurity
- Problematic supply chain transparency and efficiency

**Supply Chain Dependency Vulnerabilities**

- Lack of visibility of supply chain beyond tier one (extended supply chain)
- Inability of monitoring of long or complex chains from the entity or the competent authority
- Unwanted strategic external dependencies, including ICT concentration, in relation to ICT products and ICT services
- Limited domestic capability to develop and maintain critical ICT infrastructure, leading to over-reliance on foreign suppliers
- Limited or no strategic stockpiling of critical components
- Dependency on proprietary technologies meaning that they often do not integrate well with other systems, making it difficult to switch suppliers as well as finding effective security measures to mitigate the risks stemming from these proprietary solutions

- Supplier-specific solutions may not adhere to open standards, resulting in security through obscurity, compatibility issues with other technologies and reducing flexibility
- Supplier lock-in/dependencies or limited or no supply chain diversification or monodependencies[53], reliance on single source suppliers
- Lack of trustworthy suppliers

**Economic vulnerability**

- Cost volatility
- Cost to swap out suppliers
- Resource constraints as a result of company size

**Supplier vulnerabilities specific to the legal jurisdiction of a third country**

- Strong link between the supplier and a government of a given third country
- Lack of regulatory compliance from the provider in a third country
- Ineffective enforcement of the EU law in a third country or weak anti-corruption laws, lack of regulatory oversight, weak intellectual property considerations
- Third country's legislation, especially where there are no legislative or democratic checks and balances in place; in the absence of security or data protection agreements between the EU and the given third country; foreign laws that can have negative impact, e.g. to undermine competition and free market protections such as the requirement to transfer technology and intellectual property to domestic providers in a foreign country
- Ability for the third country to exercise any form of pressure, including in relation to the place of manufacturing of the equipment: product supervised, controlled or manipulated by a state authority; relevant for countries democratic deficit
- Third countries conducting an offensive cyber policy

[53] There is currently a gradual specialisation of organisations operations seen in most sectors, resulting in certain operations and support functions being outsourced. This in turn results in more and more ICT supply chains being established, or a number of suppliers having an increasing number of customers, thus creating a web of an increasing number of interconnected, interdependent actors. This development may result in supply chain "nodes" and, in some cases, monodependencies where organisations are dependent on a service that is only provided by one supplier; thus, no alternative service is available should the service in question cease to exist. An incident in one such node, would have consequences for all, or many, of the node´s users.

# Annex 3: Examples of impacts relevant to ICT supply chains

### Data leakage, loss or tampering (confidentiality, integrity)

- Compromise of customer data (e.g., leaked credentials, sensitive documents)
- Leakage of sensitive data (e.g., customer records, intellectual property)
- Potential breaches in data confidentiality due to non-compliance with agreed-upon security protocols
- Unauthorised access to sensitive government data, intellectual property, and personal information of citizens
- Data alteration or insertion of counterfeit data

### Financial impact or loss

- Customers' potential financial losses
- Financial losses (due to disrupted operations, delayed product delivery, and supply chain interruptions)
- Financial loss associated with mitigating the breach, restoring services, and compensating affected individuals
- Ransom demands issued by the attackers to customers
- Increased retraining costs and adaptation time in order to transition to a new supplier
- Downtime affects productivity and revenue
- High costs due to transitioning to a new supplier
- Stringent or onerous contract terms for the user, including higher prices and reduced flexibility in service agreements
- Re-evaluation of supplier relationships
- Reduced productivity, disrupted services, and revenue losses impact the Growth Domestic Product (GDP)

### Reputational damage

- Reputational damage due to the breach and loss of trust of customers
- Reputational damage at a national level
- Frustration among employees and customers

**Impact on service quality or disruption (availability, integrity)**

- Prolonged service disruption, affecting productivity and revenue
- Operational disruptions due to unauthorised activities, system instability, or service interruptions
- Disruptions or damage of critical services such as telecoms, transport, health and energy
- Intentional disruption of critical services such as healthcare, energy, transportation, and financial systems.
- Delays in service delivery
- Operational impact or cybersecurity risks due the transition to a new supplier, or due to the supplier's inability to perform regular security audits and updates as per the contract
- Delays in delivery of raw materials, components, consumer goods and services
- Emergency services, businesses, and citizens experience communication gaps
- Destruction of manufacturing plants, warehousing and distribution locations
- Data unavailability
- Reduced performance of counterfeit parts or reduced performance of the end product
- Altered or misleading service data shared or unauthorized changes to service behaviour

**Legal repercussions**

- Legal and regulatory scrutiny
- Legal actions, compensation claims, and product recalls
- Stringent contract terms for the user, including higher prices and reduced flexibility in service agreements
- Re-evaluation of supplier relationships

**Geopolitical and strategic national impacts**

- National security risks/implications
- Espionage

**Impact on public safety**

- Safety implications depending on the sector, including loss of life or implications to health

**Political impact**

- Geopolitical tension due to the perceived negligence and lack of cooperation
- Subtle manipulation of data and communication flows to undermine public trust, spread disinformation, or influence political processes.

## Annex 4: Lifecycle phases

Potential interventions, weaknesses and vulnerabilities can arise at any stage of the ICT product or service life cycle and throughout the supporting supply chain. The following is a short description of the different phases considered for the ICT Supply Chain Security Toolbox.

The **design phase** of the ICT life cycle is where the initial concepts and specifications for a product, system, or service are developed. The decisions made during this phase lay the foundation for subsequent stages, including development, manufacturing, and deployment. The design phase significantly impacts the overall efficiency, security, and sustainability of the supply chain. This crucial stage involves defining the architecture, functionality, and features, identifying the necessary components and materials, and setting standards for performance, security, and quality. It is critical to address potential vulnerabilities at this stage, as flaws introduced here – whether unintentional or malicious – can compromise the security and functionality of products that may be deployed in millions of units.

The **development and production phase** is where a designed product, system, or service is transformed from concept to reality. This phase involves translating design specifications into a functional product through coding, integrating software and hardware components, testing for functionality and security, and refining the product to meet specified requirements. It also includes the mass manufacturing process, which encompasses sourcing materials and components, assembling the product, conducting quality assurance testing, and scaling up production to meet demand. Vulnerabilities can inadvertently be introduced during this phase, potentially becoming costly to fix if not identified in early testing. Additionally, even well-designed products can have malicious components introduced during manufacturing and assembly, making these issues difficult to detect and address.

The **distribution phase** involves the processes and activities required to deliver the final product, system, or service from production facilities to end users or retailers. This phase includes packaging, warehousing, logistics, and transportation, ensuring that the product arrives safely, efficiently, and in good condition. It also covers inventory management, order fulfilment and the coordination of shipping routes and methods.

Effective distribution is essential for maintaining product quality, adhering to delivery schedules, and optimising costs. Additionally, this phase includes implementing security measures to protect against tampering, theft, and other risks during transit. Often, components transported between production facilities and customers are not managed by the personnel responsible for their design and production. Vulnerabilities introduced during this phase are more likely to be malicious and typically affect a limited number of components and customers compared to earlier phases.

The **acquisition phase** is the stage where end users or organisations purchase and receive the final product, system, or service. This phase involves selecting suppliers, negotiating contracts, and making procurement decisions. It includes assessing the product's compliance with technical specifications, security requirements, and regulatory standards. Additionally, the acquisition phase involves evaluating the total cost of ownership, which encompasses the purchase price, installation, maintenance, and potential upgrade costs. Ensuring proper documentation and warranties, as well as planning for seamless integration into existing systems, are also key aspects of this phase. Effective acquisition ensures that the purchased products meet the desired quality, functionality, and security standards and are delivered on time and within budget. Vulnerabilities introduced during this phase typically affect a limited number of customers.

The **deployment phase** of the ICT life cycle is the stage where the final product, system, or service is installed, configured, and activated at the end user’s location or within their operational environment. This phase encompasses delivery, setup, integration with existing systems, and user training. It ensures that the product is correctly implemented, operates as intended, and meets all user requirements and specifications. Additionally, the deployment phase involves verifying adherence to security protocols and operational standards, resolving any issues that arise during setup, and providing ongoing support for smooth operation and maintenance. Effective deployment is crucial for ensuring that the product or service delivers its intended value and performance in a real-world setting. During this phase, there is a risk of vulnerabilities being introduced, whether through malicious insiders inserting vulnerabilities or replacing equipment with compromised components. While such

vulnerabilities typically affect a limited number of customers, their impact can be significant.

The **maintenance** involves ongoing activities to ensure the continued functionality, performance, and security of a product, system, or service after deployment. This phase includes routine tasks such as monitoring system performance, applying software updates and patches, performing repairs, and conducting preventive maintenance to address potential issues before they escalate. It also encompasses troubleshooting and resolving operational problems, ensuring compliance with evolving security standards, and providing user support. Effective maintenance is crucial for sustaining the reliability and efficiency of the ICT product or service throughout its operational life. It helps minimise downtime and extends the overall lifespan of the system. During this phase, ICT components can be vulnerable to risks introduced through physical or network access and from exploitation of previously unknown or unpatched vulnerabilities. While maintenance-related vulnerabilities may be targeted at specific entities, they can potentially impact a broad user base, especially in the case of software updates.

The **disposal/decommissioning phase** is the stage where end-of-life products, systems, or services are safely and responsibly removed and disposed of. This phase encompasses data wiping, secure destruction of hardware, recycling, and adherence to environmental regulations and industry standards. Key activities include erasing sensitive data to prevent unauthorised access, dismantling or recycling components to minimise environmental impact, and managing electronic waste (e-waste) in compliance with legal and ethical guidelines. Effective disposal is essential for protecting data security, reducing environmental harm, and meeting regulatory requirements. Improper disposal of ICT components can expose sensitive company or customer information, while malicious actors might attempt to refurbish and resell components as new. Additionally, used parts may be less reliable, prone to failure, or potentially having malware installed.

## Annex 5: Information sharing: Traffic Light Protocol

Conditions for information sharing are guided by Traffic Light Protocol (available at https://www.first.org/tlp/). The assigned traffic light colour determines the conditions for further use.

| Color | Condition |
|---|---|
| **TLP: RED** | For the eyes and ears of individual recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. |
| **TLP: AMBER+STRICT** | Restricts sharing to the organization only. |
| **TLP: AMBER** | Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. |
| **TLP: GREEN** | Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community. |
| **TLP: CLEAR** | Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction. |