Second report on Member States' Progress in implementing the EU Toolbox on 5G Cybersecurity

June 2023

NIS COOPERATION GROUP

Table of contents

1. Introduction

1.1. Policy context

The EU Toolbox on 5G cybersecurity[1] (EU Toolbox) published in January 2020 aims to address risks related to the cybersecurity of 5G networks. It identifies and describes a set of strategic and technical measures, as well as corresponding supporting actions to reinforce their effectiveness, which may be put in place in order to mitigate the identified risks. Member States are currently implementing the different measures at national level.

The Toolbox and its key recommendations have been endorsed by the European Commission and Member States at the highest level. In October 2020, the European Council called on the EU and the Member States *"to make full use of the 5G cybersecurity Toolbox adopted on 29 January 2020, and in particular to apply the relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessment, based on common objective criteria"*[2]. In its Recommendation of December 2022, the Council of the EU reiterated that *"it is important that the Member States achieve the implementation of the measures recommended in the EU Toolbox on 5G cybersecurity and in particular that the Member States enact restrictions on high-risk suppliers, considering that a loss of time can increase vulnerability of networks in the Union"*[3]*.*

The coordinated action on 5G cybersecurity at EU-level and the EU Toolbox are part of a broader European framework for the protection of electronic communications networks and other critical infrastructures, and complements existing measures such as the European Electronic Communications Code (EECC)[4], the Telecoms Framework, the Cybersecurity Act[5], and the Directive on security of network and information systems (NIS Directive)[6].

The first report on Member States' progress in implementing the EU Toolbox was published in July 2020[7] (first Progress Report) and gave a state of play of the implementation of the different measures by Member States as of June 2020. The report concluded that concrete steps had been taken to implement the EU Toolbox. Many Member States had already adopted or were well advanced in the preparation of more advanced security measures on 5G cybersecurity. However, work was still ongoing in many Member States on defining the content and scope of the measures and in some cases, political decisions still needed to be made in this regard.

[1] 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

[2] Special meeting of the European Council (1 and 2 October 2020) – Conclusions, EUCO 13/20.

[3] Council Recommendation 15623/22 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure, 9 December 2022.

[4] Directive (EU) 2018/1972 of the European Parliament and the Council establishing the European Electronic Communications Code.

[5] 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 and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[6] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[7] NIS Cooperation Group, Report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity, 24 July 2020, https://digital-strategy.ec.europa.eu/en/library/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity

As regards 5G deployment, all EU countries have commercial 5G service available at least in a part of the country in April 2023 and approximately 81% of the EU's population is covered by at least one operator offering 5G services[8].

1.2. Objectives and content of the report

This document is the second report on the implementation of the EU Toolbox. Its main objective is to provide an overview of the EU Toolbox implementation process by Member States until May 2023, and the progress made since the first Progress Report of 2020. It has been prepared and agreed by the NIS Cooperation Group, with the support of the Commission and the EU Agency for Cybersecurity (ENISA).

The report covers the implementation of the strategic and technical measures of the EU Toolbox. Strategic Measures (SMs) include measures concerning increased regulatory powers for authorities to scrutinise network procurement and deployment, specific measures to address risks related to non-technical vulnerabilities, as well as possible initiatives to promote a sustainable and diverse 5G supply and value chain in order to avoid systemic, long-term dependency risks. Technical Measures (TMs) include measures to strengthen the security of 5G networks and equipment by addressing the risks arising from technologies, processes, human and physical factors. The report also gives an overview of the ongoing strands of work on 5G cybersecurity at EU level.

Specifically, based on the information gathered, the report provides the status of implementation of the EU Toolbox measures, an overview of national measures adopted or planned, and key findings of the analysis. In its Special report from January 2022[9], the European Court of Auditors (ECA) concluded that progress has been made to reinforce the security of 5G networks since the EU Toolbox was adopted, with a majority of Member States applying or in the process of applying restrictions on high-risk suppliers. However, the Court also highlighted that Member States applied divergent approaches regarding the use of equipment from high-risk suppliers or the scope of the restrictions, and that there is a risk that the EU Toolbox in itself cannot guarantee that Member States address security aspects in a concerted manner. This report also implements the recommendation of the European Court of Auditors (see section 4).

1.3. Methodology

The results of this report are based on information provided by Member States in the framework of the NIS Cooperation Group Work Stream on 5G Cybersecurity. This information was gathered between June 2022 and May 2023, notably through a questionnaire to which all Member States provided answers, and through further inputs and discussions during meetings of the NIS 5G Work Stream.

The level of information gathered is more detailed than in July 2020, since several Member States adopted legislation or published draft legislations since then. However, not all Member States shared detailed information on individual measures for the purpose of this report, for different reasons (decisions still being discussed/consulted or pending a political decision, national security reasons). Therefore, in several instances, the lack of information available at the time of writing this report limited the analysis that can be made on substance.

[8] 5G Observatory, Quarterly Report 18, April 2023.

[9] European Court of Auditors, Special Report 03/2022 '5G roll-out in the EU: delays in deployment of networks with security issues remaining unresolved'.

2. Member States' progress in implementing the EU Toolbox measures

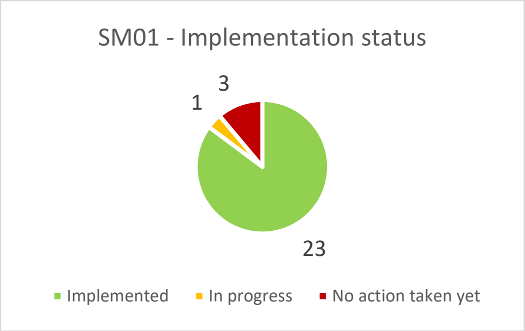
2.1. Implementation of Strategic Measures

Further progress was made in the implementation of the key strategic measures of the EU Toolbox. However, there are still differences in the state of implementation among the various measures and among Member States, which will be further detailed in the next sections, based on the data provided by Member States.

Implementation status Strategic measure	Implemented	In progress	Planned	No action taken yet
SM01	23	1	/	3
SM02	18	8	/	1
SM03	*Member States with adopted legislation:* 21	*Member States with legislation under adoption or preparation:* 3	/	*No action taken yet:* 3
	Member States with actual restrictions in place: 10	*Member States currently working on the implementation of the national legislation:* 3	/	*Member States with no restrictions in place or under preparation:* 14
SM04	12	6	/	9
SM05	9	1	1	16
SM06	3	4	2	18
SM07	See section 2.1.7.			

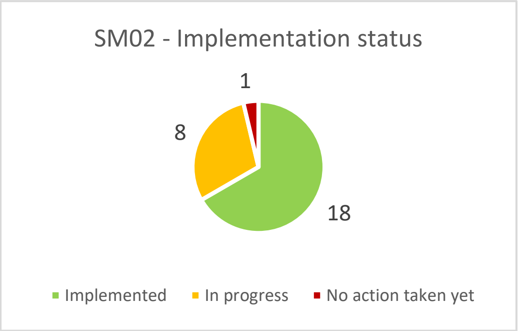
2.1.1. SM01 - Strengthening the role and powers of regulatory authorities

Measures aimed at strengthening the role of national authorities are either already implemented or in progress in twenty-four Member States. This points to a substantial increase since the first Progress Report of July 2020, when only six Member States considered this measure as implemented, and fourteen in progress, suggesting that most of the Member States which then reported ongoing or planned implementation have completed it in the meantime.



(See more detailed information concerning regulatory powers to restrict the use of 5G equipment under section 2.1.3 on SM03).

2.1.2. SM02 - Performing audits on operators and requiring information



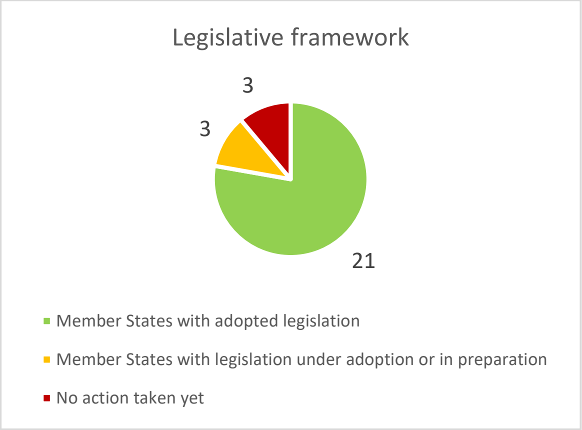
Based on Member States' replies, eighteen Member States reported having implemented SM02, while eight Member States reported the implementation to be in progress or planned. By comparison, in the first Progress Report, seven Member States indicated that this measure had been implemented and fifteen indicated that its implementation is in progress or planned.

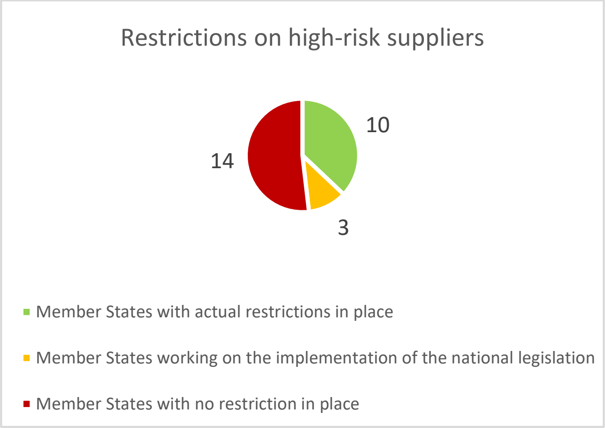
In most cases, Member States implement SM02 through the transposition of the EECC. In January 2023, twenty-five Member States have notified the Commission about complete transposition of the EECC. Sixteen Member States reported having reinforced the regulatory framework for audits and eighteen Member States are performing audits on a regular basis with the average periodicity for audits varying from every four months to every two years.

Based on the replies received, ten Member States require information on mobile network operators' (MNOs) plans for 5G equipment sourcing and for the involvement of third-party suppliers. In some Member States, this information has to be provided as part of the MNOs' risks analyses or diversification strategies reports which have to be submitted to competent authorities, or as part of the authorisation process mentioned in SM01.

2.1.3. SM03 - Restrictions for high-risk suppliers

According to SM03, Member States should have a legislative framework in place for national authorities to be able to assess the risk profile of suppliers and apply restrictions/exclusions on this basis. Secondly, it recommends to concretely perform the assessment of the risk profile of suppliers and apply restrictions, including necessary exclusions, to effectively mitigate the risks for sensitive and critical assets.





Regulatory powers of national authorities

Based on Member States' replies, twenty-one Member States reported having adopted legislation that give national authorities powers to restrict high-risk suppliers and three have legislation under adoption or in preparation[10]. However, some Member States provided limited information on the nature and content of the legislation in preparation.

[10] In preparation where a draft text from the government is under consultation.

Among them, five Member States have a pre-authorisation system/mechanism whereby MNOs have to request an authorisation to competent authorities to be able to deploy 5G equipment. This mechanism will enable other strategic measures related to supply chain risks. Four Member States reported that an advisory body has been or will be set up to advise and prepare the basis for the decision-making regarding high-risk suppliers at political level.

Twenty-one Member States reported having or developing a list of criteria to assess the risk profile of suppliers. In most cases, these criteria are public and based on the ones recommended in the EU Toolbox. The EU Toolbox recommends that Member States should make this assessment on the basis of a list of criteria taken from the EU's Coordinated risk assessment of 5G networks[11]. Such criteria include:

- The likelihood of a vendor being subject to interference from a non-EU country; for example through the existence of a strong link between the vendor and a government of a non-EU country; or through the non-EU 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 non-EU country;
- The vendor's ability to assure supply; and
- The overall quality of the vendors' products and cybersecurity practices.

The Toolbox also recommends adding country-specific information (e.g. threat assessment from national security services, etc.). In this context, several Member States have spelled out complementary criteria in their legal framework linked to:

- An offensive cyber/intelligence policy conducted by the country in which the supplier is located;
- The supplier or its country of origin being a threat to national and/or EU security.

A few other Member States have also specified other criteria, such as:

- Criteria laying down localisation requirements for the supplier[12];
- Criteria linked to the likelihood of the supplier being involved in criminal activities.

The EU Coordinated risk assessment mentioned that the corporate governance of telecom equipment suppliers presents notable differences, for example in terms of level of transparency and type of corporate ownership structure[13]. In this regard, the European Court of Auditors' Special Report on 5G contains a factual comparative analysis of 5G suppliers[14].

Out of the twenty-four Member States having legislative powers in place or under preparation, seventeen Member States have or will put in place an ex-ante approach, enabling to prohibit the deployment of 5G equipment. Nineteen Member States indicated that they are able to mandate the removal of equipment already in place provided by a high-risk supplier.

The scope of potential or actual restrictions is usually defined in national legislations, often through a list of key assets. In seventeen Member States where this scope if defined in law this list covers or

[11] 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

[12] I.e. The supplier must be located, for example, in an EU, European Economic Area (EEA), European Free Trade Association (EFTA), North Atlantic Treaty Organisation (NATO), Organisation for Economic Cooperation and Development (OECD) Member State.

[13] NIS Cooperation Group, EU-wide coordinated risk assessment of 5G networks security, 9 October 2019, see point 1.28.

[14] European Court of Auditors, Special Report 03/2022, p.33.

plans to cover assets rated as critical and highly sensitive in the EU Coordinated risk assessment, meaning that potential restrictions cover both the core and management assets and the radio access network (RAN)[15]. In ten Member States, the scope of potential or actual restrictions also identifies or plans to identify sensitive sites or geographical areas (e.g. critical infrastructure, governmental infrastructure, defence facilities, rescue systems). In addition, fourteen Member States cover or plan to cover other networks such as fixed networks, with nine Member States having a technology neutral legislation, covering any generation or type of network.

However, in practice, the actual scope of restrictions is often not yet known, as it depends on decisions not yet adopted or taken on a case-by-case basis and in some cases the decisions are made confidentially.

As for the applicability of the restrictions or potential restrictions, in twelve Member States, the legal framework that have been adopted or proposed specify transition periods, allowing time to MNOs to replace equipment from high-risk suppliers, either with specific dates (e.g. 2025) or a number of years after the entry into force of measures (on average between two and seven years after the entry into force of the law or restrictions and can vary depending on the types of network assets). In other cases, transition periods are or could be specified in the decisions taken on the basis of this legal framework.

Implementation of restrictions for the use of equipment from high-risk suppliers

Out of twenty-four Member States that have a regulatory framework in place or in preparation:

	Details	***Scope of restrictions***
Ten Member States have used these powers to impose obligations on MNOs to restrict or exclude suppliers considered as high-risk from their 5G networks.	Several Member States have taken measures to restrict the use of, or exclude, high-risk suppliers or components. In three Member States, decisions on high-risk suppliers or equipment are taken based on applications from MNOs to deploy 5G equipment. One Member State has taken a public decision to exclude Huawei and ZTE from its 5G network.	The restrictions cover both critical and highly sensitive network equipment (including the Radio Access Network) in at least six Member States. In the other four Member States, the scope of the decisions are confidential and their exact scope not known.
Three Member States are currently working on the implementation of the national legislation.		
One Member State issued a warning to critical infrastructure operators stating that equipment from two suppliers, Huawei and		

[15] Assets rated as critical in the EU Coordinated risk assessment are the core network and network function virtualisation management and orchestration (MANO). Assets rated as highly sensitive include the Radio Access Network (RAN).

ZTE, and their subsidiaries, is a cybersecurity threat.		

Market developments

In a number of Member States, one or several operators have changed suppliers when procuring 5G RAN equipment. In particular, in at least eight Member States, one or several operators have moved from one of two non-EU-controlled suppliers[16] to an EU-controlled supplier[17]. In some of cases, those changes were made before decisions about restrictions on high-risk suppliers were adopted, or in Member States where no decisions are in place yet.

On the other hand, in at least two Member States, one operator has changed from an EU to a non-EU-controlled supplier. In other cases, operators have not yet chosen their 5G suppliers.

Internal market impacts

In the context of this report and following the recommendation of the Court of Auditors[18], Member States considered the impact on the single market of a Member State building its 5G networks using equipment from a supplier considered to be high-risk in another Member State. This situation can arise if Member States take different decisions on suppliers or in the absence of assessment and decision.

The following security impacts are identified:

- The risk of spill-over is moderate to high. It is higher where MNOs provide cross-border services and in case it affects critical 5G use cases or other sectors dependent on telecoms;
- The risk of persisting dependency at Union level to potential high-risk suppliers is very high, with potential serious implications for the security of the single market and of EU's critical infrastructures.

This could also lead to a risk of negatively affecting trust in the single market. For example, this could entail the risk that services developed over 5G cannot assume a similar level of security across the internal market. It could also entail that consumers do not trust that the 5G products and services that they use are safe, or that businesses do not trust that a sufficient level of security is available across the internal market.

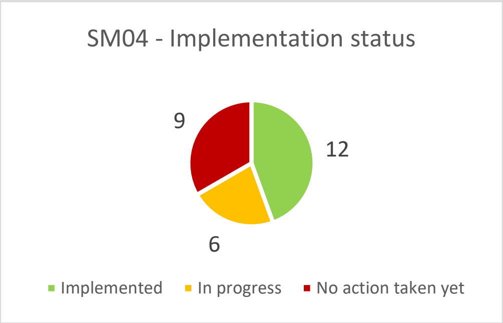
In addition, as regards economic and other impacts on operators, the Toolbox already identified a number of implementation factors when developing the EU Toolbox (notably resources costs, sector-specific economic impacts for MNOs and suppliers, broader economic and/or societal impacts). The Toolbox therefore recommends taking these factors into account when designing and implementing the measures concerning suppliers.

[16] Huawei or ZTE.

[17] Ericsson or Nokia.

[18] European Court of Auditors, Special Report 03/2022.

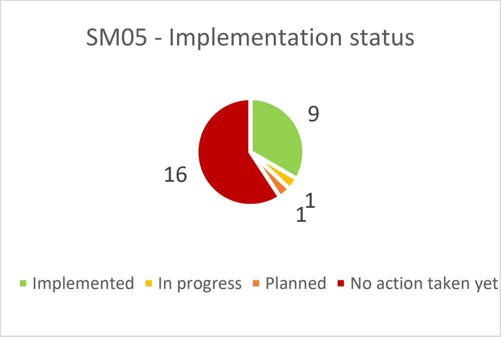
2.1.4. SM04 - Controlling the use of MSPs and equipment suppliers' third line support



Based on Member States' replies, eighteen Members States have either implemented or are in the process of implementing SM04. This indicates an increase since the first Progress Report, when five Member States considered this measure to be implemented.

In most cases, the same procedures and same restrictions for high-risk suppliers established for the implementation of SM03 also apply for the implementation of SM04. For instance, two Member States identify Managed Service Providers (MSPs) in the context of the authorisation procedure.
Four Member States reported having localisation requirements for the management of 5G services (e.g. obligation to operate mobile networks from an EU Member State), or specific requirements when they are outsourced in a third country (e.g. a national officer can be mandated to be present at the physical location of the MSP with full access to the services, or services must return to the Member State in case of emergency).

2.1.5. SM05 - Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies and avoiding dependency on high-risk suppliers

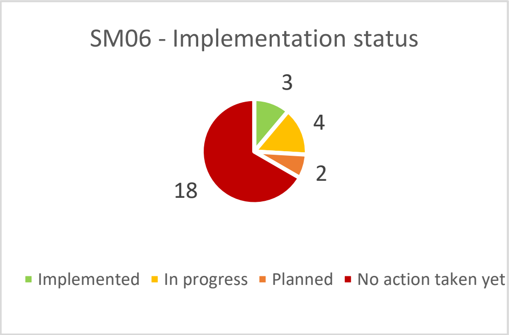


Based on Member States' replies, nine Member States reported having implemented SM05, while more than half of Member States have not. By comparison, in the first Progress Report, two Member States indicated that this measure is implemented and twelve reported that its implementation is in progress.

In these nine Member States, the competent authority is able to request information on the multi-vendor strategies of 5G MNOs or require MNOs to submit a diversification strategy. Two Member States require having a minimum number of suppliers in the different parts of the network. In one instance, the level of diversification is assessed through the authorisation system mentioned in SM01 and SM03.

As already identified in the first Progress Report, several Member States reported having difficulties implementing this strategic measure since they have a small market/country or given the interdependency of transnational operators which are regulated in their respective countries. It was also stressed that any efforts to diversify suppliers should meet the objectives of SM05 to increase the resilience and security of networks.

2.1.6. SM06 - Strengthening the resilience at national level



Similar to SM05, most Member States have no requirement to impose diversification at national level through an adequate balance of suppliers. These results are similar to the ones of the first Progress Report where only one Member State indicated that this measure is implemented, while the other Member States indicated that its implementation is planned, in progress or no action had been taken yet.

Five Member States indicated that there are no measures or implementation plans since they consider that a national dependency does not exist (e.g. because there is already an adequate balance of suppliers at national level). Similar to SM05, several Member States reported that SM06 is difficult to implement because of the small size of their national market.

2.1.7. SM07 - Screening of Foreign Direct Investment (FDI)

The EU framework for the screening of FDI became fully operational in October 2020. The Commission and Member States have worked on putting in place the necessary operational requirements for the full application of the Regulation, including:

- The notification by Member States of their existing national investment screening mechanisms to the Commission;
- The establishment of formal contact points and secure channels in each Member State and within the Commission for the exchange of information and analysis;
- Developing procedures for Member States and the Commission to quickly react to FDI concerns and to issue opinions.

By the end of 2021, twenty-five Member States either had a national FDI screening mechanism in place; adopted a new national FDI screening mechanism; amended an existing mechanism; or initiated a consultative or legislative process expected to result in the adoption of a new mechanism or amendments to an existing one[19].

2.2. Implementation of Technical Measures

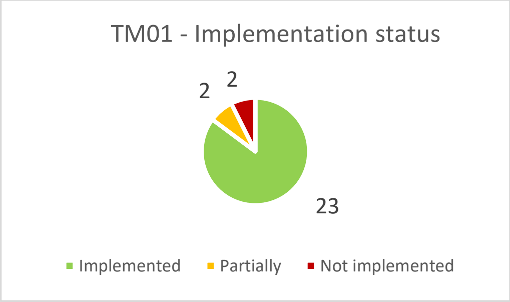
This section gives an overview of findings related to the implementation progress for TM01 to TM08 and TM11. These measures are related to the strengthening of security requirements for MNOs.

In general, based on Member States' replies, it appears that technical measures have been spelled out in national legislations. However, the scope and level of detail, as well as the level of enforcement and supervision of the measures differ substantially. For example, while some Member States reported whole sections in national regulations devoted to the implementation of a technical measure, some others appear to rely on general provisions in their legislation.

[19] Second Annual Report on the screening of foreign direct investments into the Union, COM(2022) 433 final.

Implementation status Technical measure	Implemented	Partially	Not implemented	No reply
TM01	23	2	2	/
TM02	8	5	13	1
TM03	19	4	2	2
TM04	8	5	14	/
TM05	11	7	8	1
TM06	17	6	4	/
TM07	19	5	3	/
TM08	13	6	8	/
TM09	See section 3.2.3. on standardisation and certification			
TM10				
TM11	18	6	3	/

2.2.1. TM01 - Ensuring the application of baseline security requirements

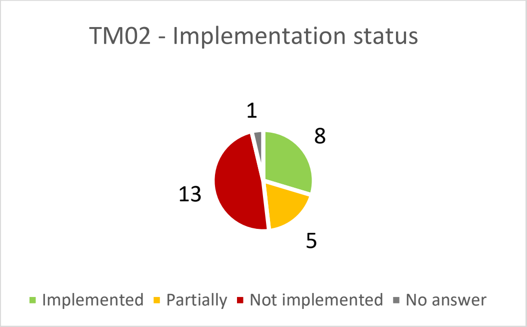


Based on Member States' replies, twenty-three Member States indicated that this measure has been implemented, and two Member States indicated its partial implementation. This would indicate an increase since the first Progress Report, suggesting that most of the Member States which then reported ongoing or planned implementation have completed it in the meantime. Nonetheless, based on the information received, two Member States do not appear to have enforceable baseline security requirements in place yet.

The reported means of implementing TM01 vary across the Member States. While some Member States rely on general security objectives, usually encapsulated in their primary legislation, most have reported more detailed measures, usually contained in regulations, directives and specific regulatory decisions. The latter group of documents often specifies various security controls to be implemented by MNOs.

In addition to legally binding measures, some Member States provide MNOs with guidelines and recommendations on their implementation. Moreover, in several Member States, MNOs either voluntarily adopted ISO/IEC 27001 certifications[20], or are in the process of doing so. Twelve Member States reported working on improving their baseline measures, or planning to do so.

2.2.2. TM02 - Implementation of security measures in existing 5G standards



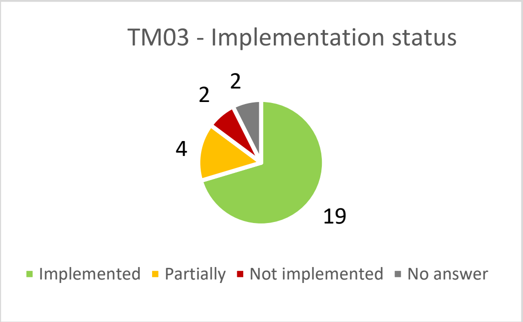
Eight Member States indicated that TM02 has been implemented, five Member States indicated its partial implementation, thirteen Member States indicated that it has not been implemented, and one Member State has not provided any information. By comparison, only two Member States reported any measures to this effect in the first Progress Report.

[20] ISO/IEC 27001 is a standard which defines requirements that an information security management systems (ISMS) must meet.

Some Member States reported carrying out periodic audits or requiring statements of compliance with specific standards and technical specifications, including the 3rd Generation Partnership Project (3GPP). Other Member States do not explicitly mandate compliance with defined standards and specifications, but nevertheless refer to them in their technical supervision activities. In other words, telecommunications networks built and configured in accordance with defined specifications would demonstrate compliance with the relevant national provisions. Finally, some Member States refer to 3GPP, European Telecommunications Standards Institute (ETSI) technical specifications and other technical and non-technical standards as means of providing guidance to the MNOs.
Five Member States reported planning on introducing or expanding national measures corresponding to TM02, in most cases focusing on 3GPP technical specifications.

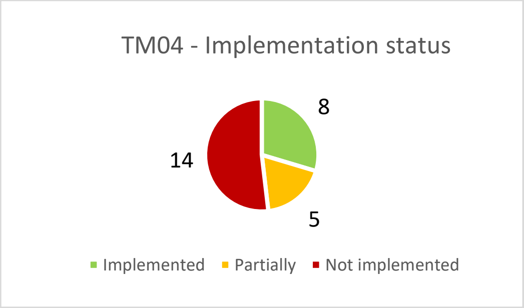
2.2.3. TM03 - Ensuring strict access controls

Nineteen Member States indicated that TM03 has been implemented, four Member States indicated its partial implementation, two indicated that it has not been implemented and two did not reply.
By comparison, seven Member States reported having this measure implemented, while in a strong majority of the Member States it was either 'in progress' or 'planned' in the first Progress Report.



There is variation in the way the Member States attempt to implement this measure. Specifically, while many Member States have more detailed measures addressing this technical measure, including provisions on access monitoring and prior background checks, there were cases of Member States reporting a general legislative obligation to apply risk-based access restrictions. A few Member States have reported enforcing the use of measures minimising or avoiding remote access by third parties.
According to the information provided, seven Member States are preparing regulatory measures to either implement or reinforce this technical measure, for example, based on ENISA Guideline on Security Measures under the EECC[21] and ISO/IEC 27000 standard family.

2.2.4. TM04 - Increasing the security of virtualised network functions



Eight Member States indicated that TM04 has been implemented, five Member States indicated its partial implementation and fourteen Member States indicated that it has not been implemented.
The above figures point to an increase since the first Progress Report, when only one Member State considered this measure as implemented. Furthermore, with eighteen Member States declaring in July 2020 that the implementation of TM04 was either in progress or at least planned, twelve of them appear to have followed through with their plans at least partially.

Similar to TM02, there are differences in the way Member States appear to view TM04 as implemented. While some Member States require conformity with Network Function Virtualisation (NFV)-specific controls, such as those based on the relevant ETSI specifications, many view the

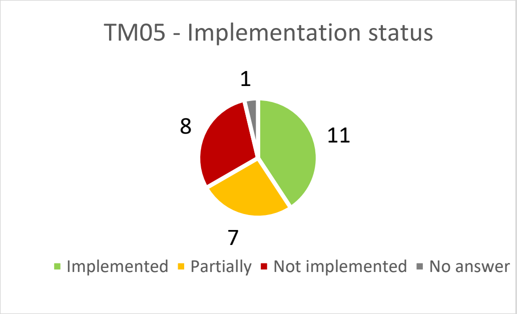
[21] ENISA Guideline on Security Measures Under the EECC, last update on 7 July 2021, https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc

implementation status of TM04 through the prism of their existing, often technologically neutral measures, for example, network segregation and patch management.

Five Member States reported looking into either implementing or further strengthening their implementation of this technical measure. In this context, in February 2022, ENISA published a report entitled 'NFV Security in 5G - Challenges and Best Practices'[22], which contents have now been incorporated into ENISA's 5G Security Controls Matrix[23], a repository consolidating security controls relevant to 5G networks and services.

2.2.5. TM05 - Ensuring secure 5G network management, operation and monitoring

Eleven Member States indicated that TM05 has been implemented, seven Member States indicated its partial implementation and eight Member States indicated that it has not been implemented. One Member State did not provide an answer. Thus, there has been an increase in the implementation of TM05 since the first Progress Report, when only four Member States considered this measure to be implemented.

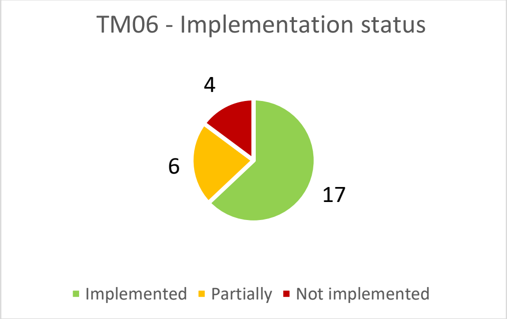


The implementation of TM05 varies across the Member States on the EU Toolbox requirement to *"Ensure that MNOs run their Network Operation Centres (NOC) and/or Security Operation Centres (SOC) on premise, inside the country and/or inside the EU"*. Most Member States do not have such explicit provisions on NOC/SOC placement. Instead, MNOs are to take decisions on NOC/SOC placement based on a risk assessment which, for example, ought to take into account legal or political context of the country from which network management tasks are carried out.

Ten Member States reported either implementing or strengthening their implementation of this technical measure, with four of them providing timelines to this effect.

2.2.6. TM06 - Reinforcing physical security

Seventeen Member States indicated that TM06 has been implemented, six Member States indicated its partial implementation and four Member States indicated that it has not been implemented. By comparison, in the first Progress Report, seven Member States indicated that this measure had been implemented. At that time, a significant majority of them also reported working on its implementation against concrete timelines.



In most cases, the reported physical security requirements were not 5G network-specific. Nevertheless, some Member States have been reviewing their measures to evaluate whether they should be updated to address 5G architecture more explicitly, for example, Multi-Access Edge Computing.

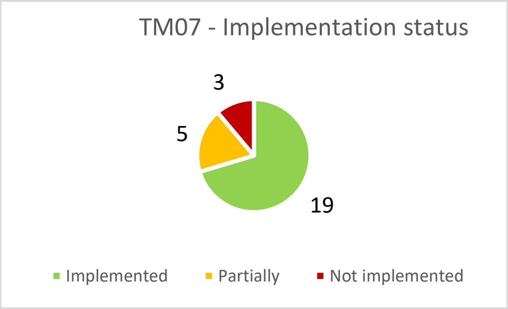
Eight Member States reported upcoming updates to this technical measure, or at least considering further refinements to it.

[22] ENISA Network Function Virtualisation Security in 5G, Challenges and Best Practices, 24 February 2022, https://www.enisa.europa.eu/publications/nfv-security-in-5g-challenges-and-best-practices

[23] ENISA 5G Security Controls Matrix, 24 May 2023, https://www.enisa.europa.eu/publications/5g-security-controls-matrix

2.2.7. TM07 - Reinforcing software integrity, update and patch management

Nineteen Member States indicated that TM07 has been implemented, five Member States indicated its partial implementation and three Member States indicated that it has not been implemented. This marks an increase since the first Progress Report, when only three Member States considered this measure implemented.

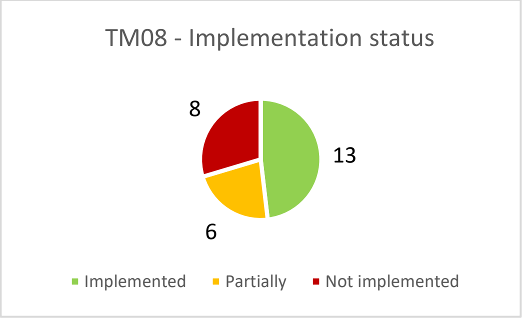


As with other technical measures, the level of detail encapsulated in national provisions varies significantly across Member States. Some of them reported higher-level security objectives of ensuring risk-based software integrity, update and patch management. Others have more detailed provisions addressing change control, testing, backup and recovery integrated into patch management, acquisition processes, identification and assurance of security requirements, as well as protection against malicious codes.

Six Member States indicated their intention to either implement or further refine their implementation of this measure, for example by reviewing it against ENISA Guideline on Security Measures under the EECC and the accompanying 5G Supplement[24].

2.2.8. TM08 - Raising security standards in suppliers' processes through robust procurement conditions

Thirteen Member States indicated that this technical measure has been implemented, six Member States indicated its partial implementation and eight Member States indicated that it has not been implemented. By comparison, five Member States reported having this measure implemented, while in most Member States it was described as either 'in progress' or 'planned' in the first Progress Report.



As with other technical measures, the level of detail varies across the measures reported by Member States. While some Member States appear to rely on higher level security objectives in their legislation, others have more detailed requirements and carry out periodic audits against this technical measure. In one Member State, MNOs need to comply with the requirements outlined in ENISA paper entitled 'Indispensable baseline security requirements for the procurement of secure ICT products and services'[25].

Six Member States reported being in the process of adopting new provisions addressing this technical measure.

2.2.9. TM09 - Using EU certification for 5G network components, customer equipment and/or suppliers' processes

See section 3.2.3. on standardisation and certification.

[24] ENISA 5G Supplement to the Guideline on Security Measures Under the EECC, last update on 7 July 2021, https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc.

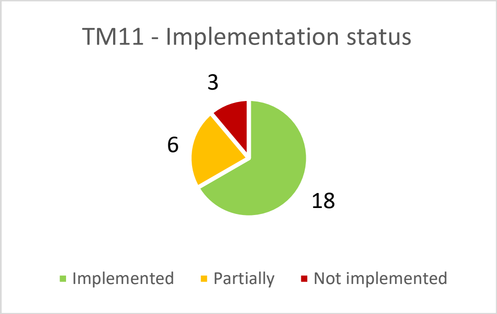
[25] ENISA Indispensable baseline security requirements for the procurement of secure ICT products and services, 21 January 2017, https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services

2.2.10. TM10 - Using EU certification for other non 5G-specific ICT products and services (connected devices, cloud services)

See section 3.2.3. on standardisation and certification.

2.2.11. TM11 — Reinforcing resilience and continuity plans

Eighteen Member States indicated that this technical measure has been implemented, six Member States indicated its partial implementation and three Member States indicated that it has not been implemented. This marks an increase since 2020, when nine Member States reported having this measure implemented fully or partially.



While most Member States have provisions on business continuity measures targeting MNOs' networks and services, there have been relatively few reported cases of these measures extending to requiring continuity within selected suppliers[26]. As with other technical measures, while some Member States reported only general requirements, others have put forward more specific provisions. The latter include fault management procedures, such as detection, response, escalation, reporting, as well as business continuity management, including service availability and continuity of provision, contingency planning and disaster recovery planning. Furthermore, some Member States require their MNOs to take ENISA Guideline on Security Measures under the EECC and the accompanying 5G Supplement into utmost account when implementing their continuity policies.
Four Member States have reported working on expanding their business continuity provisions.

3. EU Toolbox supporting actions and other EU level actions

This chapter gives an overview of some of the EU Toolbox Supporting Actions (SAs) and other activities undertaken at EU level in the field of 5G cybersecurity.

As foreseen in the Commission Recommendation on the Cybersecurity of 5G networks from March 2019[27], the Commission reviewed the impacts of the Recommendation of December 2020[28]. The review looked back at the various steps achieved and how Member States perceived the process initiated by the Recommendation. It also described the state of play of the supporting actions undertaken by the Commission and ENISA, in the fields of standardisation and certification, EU funding for secure 5G roll-out, actions to promote EU capacities in the area of network technology, and fostering a diverse and sustainable 5G ecosystem in the EU.

The conclusions of this review led to the identification of key objectives and specific actions for the future coordinated work at Union level on 5G cybersecurity, set out in the EU's Cybersecurity Strategy for the Digital Decade[29]. These objectives consist of 1) Ensuring convergent national approaches for

[26] TM11 provides that 'MNOs should request similar arrangements within their suppliers and only use suppliers who demonstrate sufficient levels of long-term resilience.'

[27] Commission Recommendation on the Cybersecurity of 5G networks, C(2019) 2335 final.

[28] Commission Report on the impacts of the Commission Recommendation 2019/534 of 26 March 2019 on the Cybersecurity of 5G networks, SWD(2020) 357 final.

[29] Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, JOIN (2020)18.

effective risk mitigation across the EU; 2) Supporting continuous exchange of knowledge and capacity building; and 3) Promoting supply chain resilience, and other EU strategic security objectives, by notably:

- Continuing and intensifying the exchange of information and best practices on specific strategic and technical measures;
- Monitoring the evolutions in the 5G technology, its architecture, the threats associated to it and organising knowledge building activities on various topics;
- Making use of the EU funding opportunities to support the Toolbox implementation;
- Defining and implementing a concrete action plan to enhance EU representation in standard setting bodies;
- Preparing a candidate certification scheme for key 5G components and suppliers' processes;
- Investing into research and innovation (R&I) capacities, and ensuring the secure roll-out of 5G networks through relevant security requirements in EU funding programmes;
- Responding to request by third countries who would like to understand and potentially use the Toolbox approach developed by the EU.

3.1. Exchange of knowledge and capacity-building

As foreseen in Supporting Action 06[30], Member States continue to regularly exchange information and best practices on the implementation of the EU Toolbox within the NIS Work Stream on 5G Cybersecurity, to promote coordination at Union level and further alignment of approaches.

In addition, ENISA has produced several guidelines on cybersecurity measures for telecom security regulatory authorities[31], as envisaged in Supporting Actions 01, 04 and 09[32]. The majority of the Member States use them to varying degrees. In some cases, ENISA guidelines are used directly as a basis for national soft law or legal instruments for security requirements for operators and/or for audit guidance. ENISA has also produced several reports on different aspects of 5G security, which support national authorities in the implementation of some of the EU Toolbox measures (e.g. Updated Threat Landscape for 5G Networks[33], Report on security controls in 5G specifications[34], Report on Network Function Virtualisation security[35] and an analysis of 5G cybersecurity standards[36]). ENISA has also developed a 5G Security Controls Matrix which consolidates various security controls into a single dynamic online repository[37].

[30] SA06: Exchange of best practices on the implementation of strategic measures, in particular national frameworks for assessing the risk profile of suppliers.

[31] ENISA Guideline on Security Measures Under the EECC, last update on 7 July 2021, and ENISA 5G Supplement to the Guideline on Security Measures Under the EECC, last update on 7 July 2021.

[32] SA01: Reviewing or developing guidelines and best practices on network security; SA04: Developing guidance on implementation of security measures in existing 5G standards; SA09: Enhancing cooperation, coordination and information sharing mechanisms.

[33] ENISA Threat Landscape for 5G Networks Report, updated on 14 December 2020, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks.

[34] ENISA Security in 5G Specifications - Controls in 3GPP, 24 February 2021, https://www.enisa.europa.eu/publications/security-in-5g-specifications.

[35] ENISA Network Function Virtualisation Security in 5G, Challenges and Best Practices, 24 February 2022.

[36] ENISA 5G Cybersecurity Standards – Analysis of standardisation requirements in support of cybersecurity policy, 16 March 2022, https://www.enisa.europa.eu/publications/5g-cybersecurity-standards.

[37] ENISA 5G Security Controls Matrix, 24 May 2023.

3.2. Supply chain resilience

3.2.1. Cybersecurity of Open Radio Access Networks (Open RAN)

On 11 May 2022, Member States, with the support of the Commission and ENISA, published a report on the cybersecurity of Open RAN[38], which will in the coming years provide an alternative way of deploying the radio access part of 5G networks based on open interfaces.

The report identified a number of potential opportunities associated with Open RAN, that could materialise if certain conditions are met. Through greater interoperability among RAN components from different suppliers, Open RAN holds perspectives for allowing greater diversification of suppliers within networks in the same geographic area. In addition, Open RAN could also bring improvements as regards:

- Visibility of the network thanks to the use of open standards and open interfaces, which could also facilitate auditing and security testing;
- Automation through the introduced intelligence in Open RAN which could help to decrease threats related to human error (this is a general trend in the evolution of network technology, not exclusive to Open RAN);
- Virtualisation and cloud-based solutions which allow for greater flexibility and make managing network resources easier (this is a general trend in the evolution of network technology, not exclusive to Open RAN).

However, the Open RAN concept still lacks maturity and cybersecurity remains a significant challenge. Especially in the short term, by introducing a new approach, new interfaces and new types of RAN components potentially coming from multiple suppliers, Open RAN would exacerbate a number of the security risks of 5G networks and expand the attack surface in the radio access part of the network. The severity of these risks will vary depending on the market impact of Open RAN and the scale of its deployment by MNOs. Specifically, key risks that are amplified or brought by Open RAN include:

- More entry points for malicious actors, irrespective of the supplier, due to a potentially increased number of suppliers and components;
- An expanded threat surface and a more complex environment leading to higher risks of vulnerability or failure, which could also lead to undesirable data and information flow to new third-party applications;
- An increased risk of misconfiguration of networks;
- Technical specifications, such as those developed by the O-RAN Alliance, not sufficiently mature and secure by design, and deficiencies in the O-RAN Alliance governance;
- New or increased dependency on cloud service/infrastructure providers, as virtualisation and the use of cloud is becoming more widespread in the telecoms sector, in particular in Open RAN deployments;
- New potential risks and impact on other network functions due to resource sharing and in case of not sufficient controls in place;
- The risk profile of a (potentially higher number of) individual suppliers continues to be an important source of vulnerabilities;
- In addition, by increasing momentum for new market players, including large non-EU players, Open RAN could have major disruptive impacts on EU capacities in the 5G supply market. This could lead to new critical dependencies in the medium to long term or to increasing existing ones (e.g. in the area of components and cloud) and weaken the EU's strategic autonomy and security.

[38] NIS Cooperation Group, Report on the cybersecurity of Open RAN, 11 May 2022, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-open-radio-access-networks

The report recommends a set of actions to help mitigate these risks and a cautious approach to deploying this new architecture. These actions include:

- Using regulatory powers to be able to scrutinise large-scale Open RAN deployment plans from MNOs and if needed, restrict, prohibit and/or impose specific requirements or conditions for the supply, large-scale deployment and operation of the Open RAN network equipment;
- Reinforcing key technical controls such as authentication and authorisation, and adapting the monitoring design to a modular environment where each component is monitored;
- Assessing the risk profile of Open RAN providers, external service providers related to Open RAN, cloud service/infrastructure providers and system integrators, and extending the controls and restrictions on MSPs to those providers;
- Addressing deficiencies in the development of technical specifications: the process should satisfy the WTO/TBT founding principles for the development of international standards and security deficiencies should be addressed;
- Including Open RAN components into the future 5G cybersecurity certification scheme, currently under development, at the earliest possible stage.

The report concludes that a cautious approach to moving towards this new architecture is recommended. Any transition from and coexistence with existing, reliable technologies should be done by allowing sufficient time and resources to assess risks in advance, implement appropriate mitigations and clearly define responsibilities in case of failure or incident. While looking for cost/performance trade-offs through Open RAN, MNOs and other stakeholders should pay sufficient attention to ensuring security, which may require significant investments, on top of existing 5G security measures.

3.2.2. Risk assessment on the cybersecurity and resiliency of Europe's communications infrastructures and networks

Following a call from EU Telecommunications Ministers to reinforce the EU's cybersecurity capabilities[39], Member States within the NIS Cooperation Group are currently conducting a risk assessment on the cybersecurity and resiliency of Europe's communications infrastructures and networks, together with the Commission and ENISA, and in close cooperation with the Body of European Regulators for Electronic Communications (BEREC). The risk assessment covers a broad range of networks and technologies and focuses on the risks of cyber-attacks on the EU's communication networks and infrastructure (as well as physical attacks on the networks and information systems, in line with the all-hazard approach of the NIS 2 Directive[40]), by a hostile third country. The results of this work will lead to recommendations and will help to define further measures, potentially covering all parts of 5G networks and all types of networks (e.g. legacy and fixed). In its Recommendation of 9 December 2022, the Council invited the NIS Cooperation to accelerate the ongoing work on this risk assessment and present first recommendations as soon as possible[41].

3.2.3. EU coordinated risk assessments beyond 5G

Looking beyond 5G, the NIS 2 Directive provides the possibility for the NIS Cooperation Group, in cooperation with the Commission and ENISA to conduct coordinated security risk assessments of

[39] Informal meeting of the Telecommunications Ministers, Nevers Call to Reinforce the EU's Cybersecurity Capabilities, 9 March 2022.

[40] 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.

[41] Council Recommendation 15623/22 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure, 9 December 2022.

critical supply chains, as carried out for 5G networks. To complement these coordinated supply chain risk assessments for specific ICT services, systems, or products under the NIS 2 Directive, 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[42].

In addition, the Commission, the High Representative and the NIS Cooperation Group, in coordination with relevant civilian and military bodies and agencies and established networks, are currently conducting a risk evaluation on the telecommunication and part of the energy sectors and will develop risk scenarios, as requested by the Council conclusions on the EU's Cyber posture[43].

3.2.4. Standardisation and certification

In the field of standardisation and certification, ENISA is currently working with an established ad-hoc working group of market stakeholders and Member States on a candidate certification scheme related to 5G. In addition, ENISA is continuing the work on a candidate scheme for cloud services. The Implementing Regulation for the EU Common Criteria certification scheme is also being finalised for adoption.

Pursuant to Supporting Action 03[44], the Subgroup on 5G standardisation and certification developed an Action Plan which sets out concrete actions to notably enhance European influence in standardisation and contribute to transparency about existing and future relevant standards and certification schemes. Among these actions, the Subgroup organised a workshop on 5G standardisation where some Member States presented their national approach to standardisation and different Standards Developing Organisations (SDOs) and associations active in 5G presented their respective activities and processes. This was followed by a discussion on Member States' needs to support their standardisation activities and increase the EU's influence in SDOs. The Subgroup is also following the European Telecommunications Standards Institute (ETSI) Publicly Available Specifications (PAS) procedure where a set of O-RAN Alliance specifications has been submitted for review and adoption by ETSI.

3.2.5. Investments in EU capacities in the area of network technologies

The Smart Networks and Services Joint Undertaking (SNS JU) has been established in November 2021[45]. Its mission is twofold: fostering Europe's technology sovereignty and reinforcing industry competitiveness in 6G by implementing the related research and innovation (R&I) programme leading to conception and standardisation around 2025 and boosting 5G deployment in Europe through guidance on the relevant programmes under the Connecting Europe Facility and in particular for 5G corridors. To do so, it manages an EU budget of EUR 900 million for the period 2021-2027, with the private sector contributing with additional equal resources to its activities. In December 2022, the SNS JU adopted its R&I Work Programme 2023-2024[46], announcing EUR 132 million of EU funding for its second call for proposals 2023[47] to advance 6G research in Europe and to develop test and pilot infrastructure capabilities. This second SNS call will expand on the thirty-five SNS projects[48] launched

[42] Council conclusions on ICT supply chain security, 13664/22, 17 October 2022.

[43] Council conclusions on the development of the European Union's cyber Posture, 9364/22, 23 May 2022.

[44] SA03: Supporting and shaping 5G standardisation.

[45] Council Regulation (EU) 2021/2085 of 19 November 2021 establishing the Joint Undertakings under Horizon Europe.

[46] https://smart-networks.europa.eu/wp-content/uploads/2022/12/sns_ri_wp_2023-24.pdf

[47] https://smart-networks.europa.eu/current-call-for-proposals/

[48] https://smart-networks.europa.eu/europe-scales-up-6g-research-investments-and-selects-35-new-projects-worth-e250-million/

in January 2023 that were selected from the first SNS call for proposals with an EU budget of EUR 250 million.

3.2.6. EU funding for secure 5G deployment

The Commission remains committed to secure connectivity, including 5G, in partner countries through international initiatives such as the Global Gateway. This seeks to channel EU spending on global infrastructure development to "*plug vulnerabilities, provide trusted connectivity, and build capacity in the face of natural or man-made challenges, physical, cyber or hybrid threats, and economic coercion for geopolitical aims*"[49]. In the framework of the Global Gateway, the EU Toolbox *"will guide investments in digital infrastructure".*

The Commission also introduced cybersecurity requirements that are in line with the EU Toolbox in the relevant work programmes and calls for proposals of European R&I oriented programmes, in particular Horizon Europe, the DIGITAL Europe Programme and Connecting Europe Facility.

The Recovery and Resilience Facility (RRF) Regulation[50] recalled that *"guaranteeing a high level of cybersecurity and trust in technologies is a pre-requisite for a successful digital transformation in the Union"*[51]*.* Member States were asked to include in their RRF plans *"where appropriate, for investments in digital capacities and connectivity, a security self-assessment based on common objective criteria identifying any security issues, and detailing how those issues will be addressed in order to comply with relevant Union and national law".*

Moreover, the Commission is cooperating with international financial institutions, including the European Investment Bank (EIB), to promote alignment of EU-financed projects with EU policies such as the EU Toolbox.

4. Implementation of the recommendations of the European Court of Auditors

This report also addresses the recommendations by the European Court of Auditors[52] (ECA) asking to:

- *"Provide further guidance or support actions on key elements of the EU toolbox on 5G cybersecurity, such as on criteria for assessing 5G vendors and classifying them as high-risk, and on data protection considerations";*
- *"Promote transparency on the Member States' approaches to 5G security, by monitoring and reporting on the implementation of the security measures";*
- *"Assess for which aspects of 5G networks security there is a need for specifying enforceable requirements";*

[49] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank, The Global Gateway, JOIN(2021)30 final.

[50] Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility.

[51] Recital (21) of the Recovery and Resilience Facility Regulation: "Guaranteeing a high level of cybersecurity and trust in technologies is a pre-requisite for a successful digital transformation in the Union. In its conclusions of 1 and 2 October 2020, the European Council called on the Union and its Member States to make full use of the 5G cybersecurity toolbox adopted on 29 January 2020, and in particular to apply the relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the Union coordinated risk assessments. The European Council underlined that potential 5G suppliers need to be assessed on the basis of common, objective criteria."

[52] European Court of Auditors, Special Report 03/2022.

- *"Promote a transparent and consistent approach regarding the Member States' treatment of MNOs' costs for replacing 5G equipment purchased from high-risk vendors by regularly monitoring and reporting on this issue within the implementation of the EU Toolbox on 5G cybersecurity";*
- *"Assess what the impact on the single market would be of a Member State building its 5G networks using equipment from a vendor considered to be high-risk in another Member State".*

In particular, this report implements the recommendation asking to *"promote transparency on the Member States' approaches to 5G security, by monitoring and reporting on the implementation of the security measures*" of the EU Toolbox.

As regards the recommendation asking to *"assess for which aspects of 5G networks security there is a need for specifying enforceable requirements"*, Member States, in the context of the preparation of this report, considered the need for complementary actions in order to ensure a consistent level of security and resilience of 5G networks. As far as potential enforceable requirements are concerned, some Member States stated that it is worthwhile considering enforceable measures, especially regarding technical aspects. Together with Member States through the NIS Cooperation Group and its relevant Work Streams (such as the Work Stream on 5G Cybersecurity; Work Stream on supply chain security; Work Stream on risk evaluation), in case of lack of action by Member States, the Commission will look at further actions to enhance the resilience of the internal market, including exploring possible legislative avenues, without prejudice to existing legislation that has already implemented restrictions in line with and/or based on the EU Toolbox and while respecting Member States' competence for national security.

Section 2.1.3. on restrictions for high-risk suppliers addresses the other recommendations of the ECA.

5. Key findings and conclusions

This report provides a state of play of the implementation of the various EU Toolbox measures at national and EU level, since the first Progress Report of July 2020.

A vast majority of Member States have reinforced or are in the process of reinforcing security requirements for 5G networks based on the EU Toolbox. However, some of the key measures have not been fully implemented yet in all Member States. Given the importance of the connectivity infrastructure for the digital economy and dependence of many critical services on 5G networks, Member States should achieve the implementation of the Toolbox without delay.

As regards strategic measures, the European Council highlighted the particular importance of applying *the relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessment, based on common objective criteria*"[53]. At this stage, twenty-four Member States have adopted or are preparing legislative measures giving national authorities the powers to perform this assessment and issue restrictions. Out of them, ten Member States have imposed such restrictions and three Member States are currently working on the implementation of the relevant national legislation.

This situation creates a clear risk of persisting dependency on high-risk suppliers in the internal market with potentially serious negative impacts on security for users and companies across the EU and the EU's critical infrastructure. A lack of swift actions by Member States regarding high-risk suppliers could

[53] Special meeting of the European Council (1 and 2 October 2020) – Conclusions, EUCO 13/20.

also affect over time the EU consumers and companies' trust in the internal market, and increase the risk of spill-over in case of cyber-attacks, especially where MNOs provide cross-border services and in case it affects critical 5G use cases or other sectors dependent on telecoms.

It is also essential that national authorities continue their efforts to fully implement the EU Toolbox measures as soon as possible in order to protect the EU's essential security interests, reduce critical dependencies and support the objectives of the economic de-risking strategy announced by the Commission[54].

In particular, as regards the implementation of strategic measures related to high-risk suppliers, Member States should:

- Ensure they have comprehensive and detailed information from MNOs about the 5G equipment currently deployed and about their plans for deploying or sourcing new equipment;
- In assessing the risk profile of suppliers, Member States should consider the objective criteria recommended in the EU Toolbox. In this context, it is evident that 5G suppliers exhibit clear differences in their characteristics, in particular as regards their likelihood of being influenced by specific third countries which have security laws and corporate governance that are a potential risk for the security of the Union. Furthermore, designations made by other Member States concerning high-risk suppliers should be taken into account, with a view to promote consistency and a high level of security across the Union;
- Based on the assessment of suppliers, Member States should impose restrictions on high-risk suppliers without delay, i.e. considering that a loss of time can increase vulnerability of networks in the Union and the Union's dependency on high-risk suppliers, especially for Member States with a high presence of potential high-risk suppliers[55];
- To effectively mitigate risks, Member States should ensure that the restrictions cover critical and highly sensitive assets identified in the EU Coordinated risk assessment, including the Radio Access Network;
- For types of equipment covered by the restrictions, operators should not be allowed to install new equipment. If transition periods are allowed for the removal of existing equipment, they shall be defined to ensure the removal of equipment in place within the shortest possible timeframe, taking into account the security risk of keeping equipment from high-risk suppliers in place, and should not be applied to allow the continued deployment of new equipment from high-risk suppliers.

As regards other strategic measures, it is recommended to:

- Implement restrictions for MSPs, and in case where functions are outsourced to MSPs, impose enhanced security provisions around the access that MSPs are given.
- Further discuss the applicability of SM05 and SM06, and how to best ensure that any potential diversification does not result in new or increased security risks but contributes to security and resilience.

As for the technical measures, Member States have all reported taking steps to reinforce technical requirements. The focus now should be on enforcing these measures and ensuring a strong level of supervision. Particular attention should be given to TM01 (Ensuring the application of baseline security requirements) which provides a minimum set of security requirements to be fulfilled by telecom

[54] https://ec.europa.eu/commission/presscorner/detail/en/speech_23_2063

[55] Based on the definition of 5G networks provided in the EU Commission Recommendation, the EU Toolbox also includes legacy networks elements based on previous generations of mobile and wireless communications technology such as 4G or 3G.

networks and services[56], TM08 (Raising security standards in suppliers' processes through robust procurement conditions) and the incident management aspects of TM05 (Ensuring secure 5G network management, operation and monitoring)[57]. Member States are also recommended to make use of ENISA's 5G Security Controls Matrix as a tool to support the implementation of the technical measures.

Further reinforcement of requirements and supervision of telecom operators will also take place in the framework of the implementation of the NIS 2 Directive. In addition, further reinforcement of security measures is also foreseen in the proposed Cyber Resilience Act (CRA)[58], which would require manufacturers of connectable software and hardware products intended for the EU market to ensure that such products are developed in line with security-by-default and security-by-design principles and that their security is maintained throughout their lifecycle.

To further harmonise technical aspects of the EU Toolbox, additional actions are taken through the development of a candidate certification scheme for 5G, and activities related to standardisation. In relation to this, Member States should coordinate to ensure sufficient European engagement in relevant standardisation bodies and contribute to achieving an appropriate level of convergence as regards technical measures relying on standardisation and certification.

Given the importance to enhance the effectiveness and consistency of the implementation by Member States of the EU Toolbox measures, in case of lack of action by Member States, the Commission will look at further actions to enhance the resilience of the internal market, including exploring possible legislative avenues in consultation with the NIS Cooperation Group, without prejudice to existing legislation that has already implemented restrictions in line with and/or based on the EU Toolbox and while respecting Member States' competence for national security. In this context, the results of the ongoing risk assessment of the cybersecurity of communications infrastructures and networks will also be taken into account (see section 3.2.2.).

[56] A framework such as ISO/IEC 27001 or ENISA Guideline on Security Measures Under the EECC could constitute a reference point for TM01.

[57] NOCs/SOCs "should provide clear visibility and implement effective network monitoring of at least all the critical components and sensitive part of 5G networks, to detect anomalies and to identify and avoid threats, such as, for example, threats to the core network coming from compromised user devices and IoT)."

[58] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM/2022/454 final.

6. Annex

Strategic, technical measures and supporting actions of the EU 5G Toolbox

STRATEGIC MEASURES					
Id	**Measure**	**Description**	**Related risks**	**Relevant actors**[59]	**Supporting actions**
SM01	**Strengthening the role of national authorities**	This should include regulatory powers for national authorities, to be able to: - impose strengthened obligations on operators, for example concerning the security of the signalling/management plane; - use *ex-ante* powers to restrict, prohibit and/or impose specific requirements or conditions, following a risk-based approach, for the supply, deployment and operation of the 5G network equipment, taking into account among other things: ▪ Security of critical and sensitive parts of 5G networks; ▪ Security of the equipment itself or the environment (deployment, interconnections, etc.); ▪ Risk of interference by a third country in the 5G supply chain; ▪ Risk of major dependency on a single supplier by individual MNOs or nationally ▪ Risks for national security.	R1 R2 R3 R4 R5 R6 R7	▪ Relevant authorities ▪ Operators	SA01 SA04 SA06
SM02	**Performing audits on operators and requiring information**	In exercising their powers under Article 41(2) of the EECC[60], competent authorities should: - Audit, or require audits, of MNOs, if needed at an in-depth technical level, for example of critical components and/or sensitive parts of the 5G networks;	R1 R2 R3 R4 R5 R6 R7	▪ Relevant authorities ▪ Operators	SA02

[59] This column aims at identifying the main owners of the measures, i.e. actors responsible for developing, enforcing and/or implementing a measure.

[60] For specific new use cases in 5G (e.g. small closed 5G network serving critical functions such as, for example, a harbour or a hospital network) it is recommended to evaluate whether regulatory powers apply to these new type of MNOs and if not, to assess the need to regulate them.

		- Require operators to provide detailed and up-to-date information about their plans for the sourcing of 5G equipment and for the involvement of third party suppliers; - Require operators to document and maintain a description on how the baseline technical network security measures are implemented[61].			
[redacted]					
SM03	**Assessing the risk profile of suppliers and applying restrictions for suppliers considered to be high risks- including necessary exclusions to effectively mitigate risks- for key assets**	- Establish a framework with clear criteria, taking into account the risk factors identified in paragraph 2.37 of the EU coordinated risk assessment[62] and adding country-specific information (e.g. threat assessment from national security services, etc.), for national competent authorities and MNOs to: - Perform rigorous assessments of the risk profile of all relevant suppliers at national level and/or EU level (for example jointly with other MS or other MNOs); -Based on the risk profile assessment, apply restrictions- including necessary exclusions to effectively mitigate risks- for key assets defined as critical or sensitive in the EU coordinated risk assessment report (e.g. core network functions, network management and orchestration functions, and access network functions);. - Take steps to ensure that MNOs have adequate controls and processes in place to manage potential residual risks, such as regular supply chain audits and risk assessments, robust risk management, and/or specific requirements for suppliers based on their risk profile.	R2 R5	▪ Relevant authorities ▪ Operators	SA06, SA10
SM04	**Controlling the use of Managed Service Providers (MSPs) and equipment suppliers' third line support**	Establish a legal/regulatory framework which places limit on the types of activity and conditions under which MNOs are able to outsource particular functions to Managed Service Providers (MSPs), for both physical and virtual infrastructure, including: - Applying restrictions in particular in sensitive parts of the 5G networks, such as the security and network operations functions and where MSPs are considered to be high risk suppliers within the meaning of SM03;	R2 R5	▪ Relevant authorities ▪ Operators	SA06, SA10

[61] This may include security domains such as, for example, administrative information security, personnel security, security of hardware, software and telecommunications, security of information material and usage, physical security and other.

[62] The EU coordinated risk assessment report identifies several risk factors for the assessment of a supplier's risk profile, notably: the likelihood of the supplier being subject to interference from a non-EU country (this may be facilitated by, but not limited to, the presence of certain factors, which are also listed in the EU coordinated risk assessment report); the supplier's ability to assure supply; and 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.

		- For functions outsourced to MSPs, impose enhanced security provisions around the access that MSPs are given to perform those functions. For equipment manufacturers' third line support during the design, deployment and/or operation of networks, impose strict access controls especially for critically sensitive components and/or sensitive parts of the network and in particular for suppliers considered to be high risk within the meaning of SM03.			
SM05	**Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies**	Ensure that each MNO has an appropriate multi-vendor strategy taking into account the technical constraints and interoperability requirements of the different parts of a 5G network: - To avoid or limit any major dependency on a single supplier (or suppliers with a similar risk profile); - To avoid dependency on suppliers considered to be high risk within the meaning of SM03.	R4	▪ Relevant authorities ▪ Operators	SA03, SA10
SM06	**Strengthening the resilience at national level**	Ensure that there is an adequate balance of suppliers at national level to ensure that there is resilience in case there is an incident with one operator and/or one supplier, taking into account the variations in geography and population in individual Member States.	R4	▪ Relevant authorities ▪ Operators	SA03, SA10
SM07	**Identifying key assets and fostering a diverse and sustainable 5G ecosystem in the EU**	- Build on the EU's Foreign Direct Investment screening mechanism to improve the monitoring of FDI investments across the 5G value chain (e.g. through a mapping of key 5G assets, the use of monitoring tools and exploring specific guidelines), in order to better detect foreign investments in the 5G value chain that may pose a threat to the security or public order of more than one EU MS. Critical infrastructure, public security, access to and control of information and cybersecurity are well embedded under the scope of this (FDI) Regulation, allowing the evaluation of investments taking into account factors such as the risk profile of buyers/companies. - Should dependencies along the 5G value chain arise as a result of trade distorting market behaviour by producers falling under the scope and conditions of the relevant EU anti-dumping and/or anti-subsidy rules – and should these be notified via an ad hoc complaint or in exceptional circumstances via the European Commission's own initiative – then such behaviour could be investigated and acted upon through the EU's trade defence measures.	R4	▪ EC and Member States	SA10

SM08	**Maintaining and building diversity and EU capacities in future network technologies**	Develop policies which create optimal conditions for European technological firms and foster innovation in key technology areas to promote a diverse, sustainable and secure European 5G eco-system, including by: – Developing the proposed EU Institutionalised partnership in the field of NGI/6G ("Smart Networks and Services")[63] to ensure there is a sufficient degree of diversity of suppliers and sufficient knowledge and supply capacity in the EU across the telecoms value chain; - Developing EU capacities and therefore also avoid dependencies by supporting disruptive and ambitious research & innovation. This relates to the implementation of the various EU funding programmes, in particular Horizon Europe, the Digital Europe Programme and the Connecting Europe Facility (CEF) (e.g. through initiatives such as 5G Corridors for Connected and Automated Mobility); - Bringing together knowledge, expertise, financial resources and economic actors throughout the Union, so as to overcome potential important market or systemic failures along the value chain (IPCEI), and further specific industry initiatives.	R4	▪ EC and Member States ▪ All 5G stakeholders	SA10

TECHNICAL MEASURES

Id	Measures	Description	Related risks	Relevant actors	Supporting actions
TM01	**Ensuring the application of baseline security requirements (secure network design and architecture)**	Ensure that MNOs implement existing security best practices and recommendations non-specific to 5G networks on, for instance product development, configuration, day-to-day network management, incident management, security updates[64], for instance by imposing and reviewing risk assessment plans by MNOs.	R1 R2 R3 R6 R7 R8 R9	▪ Relevant authorities ▪ Operators	SA01, SA05, SA09, SA10

[63] Proposed European Partnership for smart networks and services (Horizon Europe programme). Link to Inception Impact Assessment: https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2019-4972300_en

[64] These measures should be based on international or European standards or technical guidelines, for example the Article 13a expert group guidelines of minimum security measures (https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf)

		Ensure that MNOs keep up-to-date information on security policy, including operational information, as well as linked to change and incident management procedures for key network and information systems.			
TM02	**Ensuring and evaluating the implementation of security measures in existing 5G standards**	Ensure that MNOs and their suppliers implement the existing security measures in the relevant 5G technology standards (e.g. 3GPP)and use it as a minimum security baseline for MNOs, so as to ensure that also the optional parts of these standards, relevant for security, are adequately implemented	R1 R2 R3 R6 R7 R9	▪ Relevant authorities ▪ Operators ▪ Suppliers	SA03, SA04, SA05, SA10
TM03	**Ensuring strict access controls**	Ensure that MNOs implement adequate, flexible and verifiable technical measures to ensure that: - Strict network access controls are applied; - The principle of least privilege is applied, ensuring that various rights in the network (e.g. access rights between network functions, network administrators' rights, virtualization configuration) are minimized; - The segregation of duties principle is applied; - Procedures are in place to ensure that these rules are in effect all the time and evolve with the network. In setting the access control policies, particular care should be taken to ensure that remote access by third parties, especially suppliers considered to be high risk, is minimized and/or avoided whenever possible. When remote access is necessary, for example to address service outages, the MNO should apply appropriate authentication[65], authorization, logging and auditing so as to have a clear visibility on access to data and configuration changes or network alterations.	R1 R2 R3 R5 R6 R7	▪ Relevant authorities ▪ Operators	SA05, SA10
TM04	**Increasing the security of virtualised network functions**	Ensure that MNOs follow security best practices for network function virtualisation. Note that there may be settings, for example when a network function is highly critical or when it is handling highly sensitive information, where virtualization is not appropriate and in such settings physical separation may be necessary.	R1 R3 R6 R7	▪ Relevant authorities ▪ Operators	SA01, SA05, SA10

[65] In terms of authentication general good practices apply and appropriate mechanisms should be used, for example for temporary access by third parties and/or remote access (e.g. no permanent credentials, temporary (one-time) passwords, usable only for designated tasks should be used). These measures could, for example, be enforced by using appropriate Privileged Access Management (PAM) platforms.

TM05	**Ensuring secure 5G network management, operation and monitoring**	Ensure that MNOs run their Network Operation Centres (NOC) and/or Security Operation Centres (SOC) on premise, inside the country and/or inside the EU. The NOC and SOC are a vital component of the MNO's infrastructure in implementing and monitoring the measures for secure network management and operation. They should provide clear visibility and implement effective network monitoring of at least all the critical components and sensitive part of 5G networks, to detect anomalies and to identify and avoid threats, such as, for example, threats to the core network coming from compromised user devices and IoT). Also ensure that MNOs appropriately protect the management traffic of the communications network or service to avoid unauthorised changes to the communications network or service components.	R1 R2 R3 R5 R6 R7 R9	▪ Relevant authorities ▪ Operators	SA05, SA09, SA10
TM06	**Reinforcing physical security**	Ensure that MNOs reinforce physical protection of critical components and sensitive parts of the 5G networks, taking a risk-based approach for Multi-access Edge Computing (MEC) and base stations[66], for example considering where the components are deployed and used, like a MEC use in hospitals. In reinforcing physical access controls, it is important to ensure that access is granted only to a limited number of security-vetted, trained and qualified personnel. Access by third-parties, contractors, and employees of suppliers/vendors, integrators, should be limited and monitored, particularly where it concerns critical components and sensitive parts of the 5G networks.	R6 R7	▪ Relevant authorities ▪ Operators	SA05, SA10
TM07	**Reinforcing software integrity, update and patch management**	Ensure that MNOs deploy adequate tools and processes to ensure software integrity, which reliably identify and keep track of changes and the status of patches, when performing software updates and applying security patches in the 5G networks.	R1 R3 R5 R6 R7	▪ Relevant authorities ▪ Operators	SA02, SA10
[redacted]					

[66] When doing the risk analysis, MNOs should consider the components and the service (like critical hospital MEC service).

TM08	**Raising the security standards in suppliers' processes through robust procurement conditions**	Ensure that MNOs demand specific security standards from equipment suppliers in the procurement process (e.g. on specific security improvements and demonstrating quality levels, security maintenance of the equipment throughout its lifetime and built-in of security in the product' development processes).	R3 R6 R7	▪ Relevant authorities ▪ Operators ▪ Suppliers	SA02, SA10
TM09	**Using EU certification for 5G network components, customer equipment and/or suppliers' processes**	The Commission should consider including into the Union Rolling Work Programme[67] relevant EU-wide scheme(s) for critical network components used in the 5G networks and/or for 5G customer equipment (for example, for eSIMs and related cryptographic material) under the EU certification framework. It should also be examined at a later stage whether the certification or supplier's process could also be added to the Union Rolling Work Programme.	R3 R6 R7	▪ Relevant authorities ▪ EC ▪ ENISA ▪ Stakeholders	SA02, SA03 , SA09, SA10
TM10	**Using EU certification for other non 5G-specific ICT products and services (connected devices, cloud services)**	The Commission should consider including into the Union Rolling Work Programme EU-wide schemes under the EU certification framework for non-5G specific ICT products and services, such as for: - The security of cloud services and related technologies, which are an important part of 5G deployment[68]; - The security of connected (end-user) devices, including IoT.	R9	▪ Relevant authorities ▪ EC ▪ ENISA ▪ Stakeholders	SA02, SA03, SA09, SA10

[67] Under the EU cybersecurity certification framework, the Commission should publish the Union Rolling Work Programme for the development for the EU-wide certification schemes by July 2020.

[68] In accordance with Article 48(2) of the Cybersecurity Act, on 21 November 2019 the European Commission requested ENISA to prepare a candidate European cybersecurity certification scheme for cloud services.

TM11	**Reinforcing resilience and continuity plans**	Ensure that MNOs reinforce their resilience and continuity plans. MNOs should ensure they have adequate plans in place in case of disaster affecting the ongoing operation of their network, and ensure any critical dependencies are mapped and mitigated as required. MNOs should request similar arrangements within their suppliers and only use suppliers who demonstrate sufficient levels of long-term resilience.	R7 R8	▪ Relevant authorities ▪ Operators ▪ Suppliers ▪ Critical infrastructure operators	SA07, SA08, SA10

SUPPORTING ACTIONS

Id	Supporting action	Description	Relevant actors	Related measure(s)
SA01	**Reviewing or developing guidelines and best practices on network security**	Update the existing technical guidance on security measures for telecom providers based on Article 13a of the EU telecom framework directive and align it with Article 40 of the European Electronic Communications Code (EECC), taking also into account the need to develop best practices as regards new technologies and developments, such as Network Function Virtualisation (NFV).	▪ Relevant authorities ▪ ENISA ▪ Operators	SM01, TM01, TM04
SA02	**Reinforcing testing and auditing capabilities at national and EU level**	Reinforce competences, testing and auditing capabilities at national and/or EU level and, in particular: - Support the development of expertise of Information systems security audit service providers in telecom security audits through capacity building and EU investment in training; - The Commission should consider including into the Union Rolling Work Programme the development of an EU certification scheme for cybersecurity audit service providers in particular to support the development of capability for in-depth technical audits and security evaluations in co-operation between MS and facilitate sharing information on benchmarks of certified audit service providers. Union level framework for technical audits and security evaluation will give better position to require security from suppliers.	▪ Relevant authorities ▪ EC ▪ ENISA	SM02, TM07, TM08, TM09, TM10
SA03	**Supporting and shaping 5G standardisation**	Increase engagement in relevant standardisation bodies, in particular through reinforced coordination at EU level in order to increase ability to shape standardisation according to identified needs, by setting up a forum or group of national regulatory authorities and other	▪ Relevant authorities ▪ EC	SM05, SM06, TM02, TM09, TM10

		relevant competent authorities of Member states, reporting to the NIS Cooperation Group and the EECG[69], in particular tasked to: - Contribute to achieving an appropriate level of convergence as regards technical measures relying on standardisation and certification, in line with existing legislation, such as but not limited to the Cybersecurity Act; - Promote standardisation of interfaces to facilitate diversity of suppliers; - ensure liaison between the NIS Cooperation Group and relevant European and/or international standardisation bodies; - Ensure full participation by EU industry and improve the dialogue between the industry and the MS.	▪ Operators ▪ Suppliers ▪ ENISA	
SA04	**Developing guidance on implementation of security measures in existing 5G standards**	Develop specific EU guidance on the implementation of security measures under the existing 5G standards (e.g. 3GPP), and in particular: - Provide recommendations on the optional elements of standardisation and on aspects that are not covered by a specific standard;[70] - Identify existing gaps in telecommunications standardisation of architectures/functionalities for mitigating identified risks.	▪ Relevant authorities ▪ ENISA	SM01, TM02
SA05	**Ensuring the application of standard technical and organisational security measures through specific EU-wide certification scheme**	Consider developing an EU-wide certification scheme under the EU certification framework for information security management systems (ISMS) for telecommunication providers.	▪ Relevant authorities ▪ ENISA ▪ Stakeholders	TM01 to 06
SA06	**Exchange of best practices on the implementation of strategic measures, in particular national frameworks for assessing the risk profile of suppliers**	To facilitate a coordinated approach, exchange good practices on the implementation of strategic measures, in particular on the risk factors to be taken into account (see paragraph 2.37 of the EU coordinated risk assessment report) when assessing the risk profile of suppliers/vendors. In addition to the factors listed in the EU coordinated risk assessment report, these factors could include national-specific information such as market penetration of suppliers, threat intelligence from national security services, etc.	▪ Relevant authorities	SM01, SM03, SM04

[69] The European Cybersecurity Certification Group (EECG) set up under the Cybersecurity Act is composed representatives of national cybersecurity certification authorities or representatives of other relevant national authorities.

[70] This may include, for example, aspects such as deployment/hosting options, recommended commercial off-the-shelf (COTS) software and hardware architectures and configurations, monitoring procedures or any other aspects.

SA07	**Improving coordination in incident response and crisis management**	Through the ongoing work within the dedicated NIS Work stream, ensure there are good cooperation and coordination mechanisms between the relevant national authorities and at EU level when dealing with large-scale cross-border cybersecurity incidents and crises, on the basis of the Blueprint[71]. Moreover, to prepare for large-scale incidents involving 5G networks, Member States could consider including 5G scenarios in national as well as EU-wide cyber exercises, where appropriate.	▪ Relevant authorities ▪ ENISA	TM11
SA08	**Conducting audits of interdependencies between 5G networks and other critical services**	Analyse critical dependencies between the 5G networks and other critical sectors, such as electricity supply, as well as sectoral dependencies for 5G, such as drinking water and transportation. This should also consider circular dependencies (e.g. 5G network dependent on power supply and, at the same time, power being dependent on 5G network).	▪ Relevant authorities	TM11
SA09	**Enhancing cooperation, coordination and information sharing mechanisms**	Consider the use of existing cooperation, coordination and information sharing mechanisms, including actions and support by ENISA, notably through regular threat assessments.	▪ Relevant authorities ▪ ENISA	TM01, TM05, TM09, TM10
SA10	**Ensuring 5G projects supported with public funding take into account cybersecurity risks**	Develop detailed guidelines for 5G-related security provisions in public procurement and EU funding programmes (Horizon, Connecting Europe Facility, Digital Europe Programme). These guidelines could be prepared within the comitology procedure by committee members nominated by Member States in the course of preparing the annual work programmes under the different funding programmes. Public funding programmes such as the Connecting Europe Facility (CEF) Digital are expected to play a key role in shaping the deployment of 5G networks in Europe, e.g. 5G Corridors for Connected and Automated Mobility as well as 5G Connectivity for Socio-Economic Drivers. Therefore the above-mentioned guidelines should be used in the implementation of these programmes. In particular, when consortia for such projects are set up with participation or administrative support by public authorities, where cyber-security risks (in particular risks identified in the EU coordinated risk assessment report and the relevant mitigation measures	▪ Relevant authorities ▪ EC	SM03 to 08 TM01 to 11

[71] Commission Recommendation on a coordinated response to large-scale cybersecurity incidents & crisis (EU 2017/1584).

		described in this toolbox) are identified, those should be taken into consideration when selecting suppliers or other project participants. At national level, in the area of public procurement, the EU Directives and policies encourage Member States to not award contracts solely on the basis of the lowest price, but also take into account quality in areas such as security, labour and environmental standards. Moreover, the Commission Recommendation of 26 March 2019 refers specifically to the possible development and implementation of European cybersecurity certification schemes in public procurement related to 5G networks.		