European Parliament
2019-2024

Committee on Industry, Research and Energy

2023/0108(COD)

21.9.2023

AMENDMENTS
17 - 52

Draft report
Josianne Cutajar
(PE752.802v01-00)

Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services

Proposal for a regulation
(COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Amendment 17
Evžen Tošenovský

Proposal for a regulation
Recital 2

Text proposed by the Commission	*Amendment*
(2) Managed security services***, which*** are services ***consisting*** of carrying out, or providing assistance for, activities relating to their customers' cybersecurity risk management, have gained increasing importance in the prevention and mitigation of cybersecurity incidents. Accordingly, the providers ***of those services*** are considered as essential or important entities belonging to a sector of high criticality pursuant to Directive (EU) 2022/2555 ***of the European Parliament and of the Council***[8] . Pursuant to Recital 86 of that Directive, managed security service providers in areas such as incident response, penetration testing, security audits and consultancy, play a particularly important role in assisting entities in their efforts to prevent, detect, respond to or recover from incidents. Managed security service providers have however also themselves been the target of cyberattacks and pose a particular risk because of their close integration in the operations of their customers. Essential and important entities within the meaning of Directive (EU) 2022/2555 should therefore exercise increased diligence in selecting a managed security service provider.	(2) Managed security services are services ***provided by the managed security service providers pursuant to point (40) of Article 6 of Directive (EU) 2022/2555 of the European Parliament and of the Council. Those services consist*** of carrying out, or providing assistance for, activities relating to their customers' cybersecurity risk management, have gained increasing importance in the prevention and mitigation of cybersecurity incidents. Accordingly, the ***managed security service*** providers are considered as essential or important entities belonging to a sector of high criticality pursuant to ***point 10 of Annex I of*** Directive (EU) 2022/2555. Pursuant to Recital 86 of that Directive, managed security service providers in areas such as incident response, penetration testing, security audits and consultancy, play a particularly important role in assisting entities in their efforts to prevent, detect, respond to or recover from incidents. Managed security service providers have however also themselves been the target of cyberattacks and pose a particular risk because of their close integration in the operations of their customers. Essential and important entities within the meaning of Directive (EU) 2022/2555 should therefore exercise increased diligence in selecting a managed security service provider.
[8] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972,	[8] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972,

and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

Or. en

Amendment 18
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Recital 2

Text proposed by the Commission	*Amendment*
(2) Managed security services, which are services consisting of carrying out, or providing assistance for, activities relating to their customers' cybersecurity risk management, have gained increasing importance in the prevention and mitigation of cybersecurity incidents. Accordingly, the providers of those services are considered as essential or important entities belonging to a sector of high criticality pursuant to Directive (EU) 2022/2555 of the European Parliament and of the Council[8] . Pursuant to Recital 86 of that Directive, managed security service providers in areas such as incident response, penetration testing, security audits and consultancy, play a particularly important role in assisting entities in their efforts to prevent, detect, respond to or recover from incidents. Managed security service providers have however also themselves been the target of cyberattacks and pose a particular risk because of their close integration in the operations of their customers. Essential and important entities within the meaning of Directive (EU) 2022/2555 should therefore exercise increased diligence in selecting a managed security service provider.	(2) Managed security services, which are services consisting of carrying out, or providing assistance for, activities relating to their customers' cybersecurity risk management***, including incident prevention, detection, responce or recovery***, have gained increasing importance in the prevention and mitigation of cybersecurity incidents. Accordingly, the providers of those services are considered as essential or important entities belonging to a sector of high criticality pursuant to Directive (EU) 2022/2555 of the European Parliament and of the Council[8] . Pursuant to Recital 86 of that Directive, managed security service providers in areas such as incident response, penetration testing, security audits and consultancy, play a particularly important role in assisting entities in their efforts to prevent, detect, respond to or recover from incidents. Managed security service providers have however also themselves been the target of cyberattacks and pose a particular risk because of their close integration in the operations of their customers. Essential and important entities within the meaning of Directive (EU) 2022/2555 should therefore exercise increased diligence in selecting a managed security service provider.

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

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

Or. en

Amendment 19
Evžen Tošenovský

Proposal for a regulation
Recital 3

Text proposed by the Commission	*Amendment*
(3) Managed security services providers also play an important role in the EU Cybersecurity Reserve whose gradual set-up is supported by Regulation (EU) …/…. [laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents] The EU Cybersecurity Reserve is to be used to support response and immediate recovery actions in case of significant and large-scale cybersecurity incidents. Regulation (EU) …/…[laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents] lays down a selection process for the providers forming the EU Cybersecurity Reserve, which should, inter alia, take into account whether the provider concerned has obtained a European or national cybersecurity certification. ***The relevant services provided by 'trusted providers' according to Regulation (EU) …./…..[laying down measures to***	(3) Managed security services providers also play an important role in the EU Cybersecurity Reserve whose gradual set-up is supported by Regulation (EU) …/…. [laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents] The EU Cybersecurity Reserve is to be used to support response and immediate recovery actions in case of significant and large-scale cybersecurity incidents. Regulation (EU) …/…[laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents] lays down a selection process for the ***trusted managed security service*** providers forming the EU Cybersecurity Reserve, which should, inter alia, take into account whether the provider concerned has obtained a European or national cybersecurity certification. ***Moreover, once an European*** cybersecurity ***certification scheme for*** managed security ***service is in***

strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity ***threats and incidents] correspond to*** **'**managed security ***services'*** in accordance with ***this Regulation***.	***place, which would also replace all relevant national cybersecurity certification schemes, a compulsory certificication*** in accordance with ***that certification scheme should apply for inclusion of the trusted managed security service providers in the EU Cybersecurity Reserve***.

Or. en

Amendment 20
Johan Nissinen

Proposal for a regulation
Recital 4

Text proposed by the Commission	*Amendment*
(4) Certification of managed security services is not only relevant in the selection process for the EU Cybersecurity Reserve but it is also an essential quality indicator for private and public entities that intend to purchase such services. In light of the criticality of the managed security services and the sensitivity of the data they process, certification could provide potential customers with important guidance and assurance about the trustworthiness of these services. European certification schemes for managed security services contribute to avoiding fragmentation of the single market. This Regulation therefore aims at enhancing the functioning of the internal market.	(4) Certification of managed security services is not only relevant in the selection process for the EU Cybersecurity Reserve but it is also an essential quality indicator for private and public entities that intend to purchase such services. In light of the criticality of the managed security services and the sensitivity of the data they process, certification could provide potential customers with important guidance and assurance about the trustworthiness of these services. European certification schemes for managed security services contribute to avoiding fragmentation of the single market. This Regulation therefore aims at enhancing the functioning of the internal market. ***At the same time, these multiple purposes of the regulation should strike a balance with the potential regulatory burden and costs associated with certification, given that compliance with certification requirements will involve additional expenses and administrative efforts, which could be a concern for smaller providers.***

Or. en

Amendment 21
Ville Niinistö
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 4 a (new)

Text proposed by the Commission	*Amendment*
	(4 a) As the market and the educational systems offer variety of educational resources and formal trainings, it must be underlined that knowledge is also aquired in non-formal ways and skills can be demonstrated via degrees and certification but not exclusively. Especially in the curent fast evolving threat landscape, Member States and the beneficiaries of managed security services should take into account the highly skilled vulnerability researchers. Moreover entities and natural persons researching vulnerabilities may in some Member States be exposed to criminal and civil liability therefore Member States are encouraged to issue guidelines for non-prosecution of information security research and an exception for civil liability for those activities.

Or. en

Justification

The landscape of security professionals varies in part due to different non standardized career paths, access to formal education and resources to become certified. Therefore we need to encourage the employment of skilled people and ensure a positive framework for activities that result in an improvement of cybersecurity.

Amendment 22
Josianne Cutajar

Proposal for a regulation
Recital 4 a (new)

Text proposed by the Commission	*Amendment*
	(4 a) The Union certification scheme for managed security services should ensure the availability of secure and high quality services which guarantee a safe digital transition and contribute to the achievement of targets set up in the Path to the Digital Decade Policy Programme[8a], especially with regards to the goal that 75% of EU companies start using Cloud/AI/Big Data, that more than 90% of SMEs reach at least a basic level of digital intensity and that key public services are offered online.
	[8a] Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030

Or. en

Amendment 23
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Recital 4 a (new)

Text proposed by the Commission	*Amendment*
	(4 a) European certification schemes for managed security services should facilitate the use of these services, particularly for smaller entities, including local and regional authorities or SMEs, which often do not have the financial and human capacity to conduct these services by themselves, but are vulnerable to cyber attacks with potentially significant consequences.

Or. en

Amendment 24
Josianne Cutajar

Proposal for a regulation
Recital 5

Text proposed by the Commission	*Amendment*
(5) In addition to the deployment of ICT products, ICT services or ICT processes, managed security services often provide additional service features that rely on the competences, expertise and experience of their personnel. A very high level of these competences, expertise and experience as well as appropriate internal procedures should be part of the security objectives in order to ensure a very high quality of the managed security services provided. In order to ensure that all aspects of a managed security service can be covered by a certification scheme, it is therefore necessary to amend Regulation (EU) 2019/881. The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council and delivered an opinion on [DD/MM/YYYY	(5) In addition to the deployment of ICT products, ICT services or ICT processes, managed security services often provide additional service features that rely on the competences, expertise and experience of their personnel. A very high level of these competences, expertise and experience as well as appropriate internal procedures should be part of the security objectives in order to ensure a very high quality of the managed security services provided. In order to ensure that all aspects of a managed security service can be covered by a certification scheme, it is therefore necessary to amend Regulation (EU) 2019/881. The ***certification scheme established under this Regulation should also take into account the results and recommendations of the evaluation and review provided for under Article 67 thereof. The*** European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council and delivered an opinion on [DD/MM/YYYY

Or. en

Amendment 25
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Recital 5

Text proposed by the Commission	*Amendment*
(5) In addition to the deployment of ICT products, ICT services or ICT processes, managed security services often provide additional service features that rely on the competences, expertise and experience of their personnel. A very high level of these competences, expertise and experience as well as appropriate internal procedures should be part of the security objectives in order to ensure a very high quality of the managed security services provided. In order to ensure that all aspects of a managed security service can be covered by a certification scheme, it is therefore necessary to amend Regulation (EU) 2019/881. The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council and delivered an opinion on [DD/MM/YYYY	(5) In addition to the deployment of ICT products, ICT services or ICT processes, managed security services often provide additional service features that rely on the competences, expertise and experience of their personnel. A very high level of these competences, expertise and experience as well as appropriate internal procedures should be part of the security objectives in order to ensure a very high quality ***and reliability*** of the managed security services provided. In order to ensure that all aspects of a managed security service can be covered by a certification scheme, it is therefore necessary to amend Regulation (EU) 2019/881. The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council and delivered an opinion on [DD/MM/YYYY

Or. en

Amendment 26
Evžen Tošenovský

Proposal for a regulation
Recital 5

Text proposed by the Commission	*Amendment*
(5) In addition to the deployment of ICT products, ICT services or ICT processes, managed security services often provide additional service features that rely on the competences, expertise and experience of their personnel. A very high level of these competences, expertise and experience as well as appropriate internal procedures should be part of the security objectives in order to ensure a very high quality of the managed security services	(5) In addition to the deployment of ICT products, ICT services or ICT processes, managed security services often provide additional service features that rely on the competences, expertise and experience of their personnel. A very high level of these competences, expertise and experience as well as appropriate internal procedures should be part of the security objectives in order to ensure a very high quality of the managed security services

provided. In order to ensure that all aspects of a managed security service can be covered by a certification scheme, it is therefore necessary to amend Regulation (EU) 2019/881. The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council and delivered an opinion on [DD/MM/YYYY	provided. In order to ensure that all aspects of a managed security service can be covered by a ***dedicated*** certification scheme, it is therefore necessary to amend Regulation (EU) 2019/881. The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council and delivered an opinion on [DD/MM/YYYY

Or. en

Amendment 27
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Recital 5 a (new)

Text proposed by the Commission	*Amendment*
	(5 a) Given that the European cybersecurity schemes should certifiy that managed security services are provided by highly-skilled personnel that is able to reliably deliver these services and ensure the highest standards of cybersecurity, it is imperative that there is sufficient availability of highly-qualified personnel in the Union. Yet, the Union is faced with a talent gap, characterized by a shortage of skilled professionals, and a rapidly evolving threat landscape as acknowledged in the Commission communication of 18 April 2023 on the Cybersecurity Skills Academy. It is important to bridge this talent gap by strengthening cooperation and coordination among the different stakeholders, including the private sector, academia, Member States, the Commission and ENISA to scale up and create synergies for the investment in education and training, the development of public-private partnerships, support of

research and innovation initiatives, the development and mutual recognition of common standards and certification of cybersecurity skills, including through the European Cyber Security Skills Framework. This should also facilitate the mobility of cybersecurity professionals within the Union.

Or. en

Amendment 28
Johan Nissinen

Proposal for a regulation
Recital 5 a (new)

Text proposed by the Commission	*Amendment*
	(5 a) Given that, certification schemes will add complexity to an already complex regulatory landscape, it is of critical importance to prevent potential overlaps or conflicts with existing cybersecurity regulations and standards. Stresses further the need for careful consideration and proportionality in the implementation of the regulation, in order to reduce negative effects on market freedom and innovation.

Or. en

Amendment 29
Josianne Cutajar

Proposal for a regulation
Recital 5 a (new)

Text proposed by the Commission	*Amendment*
	(5 a) Appropriate funding and resources should be considered to accompany the additional tasks entrusted to ENISA by

this Act.

Or. en

Amendment 30
Evžen Tošenovský

Proposal for a regulation
Article 1 – paragraph 1 – point 2 – point a – introductory part

Text proposed by the Commission	*Amendment*
(a) points 9, 10 and 11 are replaced by the following:	(a) points ***7,*** 9, 10 and 11 are replaced by the following:

Or. en

Amendment 31
Evžen Tošenovský

Proposal for a regulation
Article 1 – paragraph 1 – point 2 – point a
Regulation (EU) 2019/881
Article 2 – point 7

Text proposed by the Commission	*Amendment*
	(7) 'incident handling' means incident handling as defined in point (8) of Article 6 of Directive (EU) 2022/2555;

Or. en

Amendment 32
Evžen Tošenovský

Proposal for a regulation
Article 1 – paragraph 1 – point 2 – point b – introductory part

Text proposed by the Commission	*Amendment*
(b) the following ***point is*** inserted:	(b) the following ***points are*** inserted:

Or. en

Amendment 33
Evžen Tošenovský

Proposal for a regulation
Article 1 – paragraph 1 – point 2 – point b
Regulation (EU) 2019/881
Article 2 – point 7a

Text proposed by the Commission	*Amendment*
	(7a) 'risk' means risk as defined in point (9) of Article 6 of Directive (EU) 2022/2555;

Or. en

Amendment 34
Evžen Tošenovský

Proposal for a regulation
Article 1 – paragraph 1 – point 2 – point b
Regulation (EU) 2019/881
Article 2 – point 14a

Text proposed by the Commission	*Amendment*
(14a) 'managed security service' means a ***service consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, including incident response, penetration testing,*** security ***audits and consultancy***;	(14a) 'managed security service' means a ***managed*** security ***service within the meaning of point (40) of Article 6 of Directive (EU) 2022/2555***;

Or. en

Amendment 35
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 1 – paragraph 1 – point 2 – point b

Regulation (EU) 2019/881
Article 2 – point 14a

Text proposed by the Commission	*Amendment*
(14a) ‘managed security service’ means a service consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, including incident response, ***penetration testing, security audits and consultancy***;	(14a) ‘managed security service’ means a ***managed*** service consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, including incident ***prevention, detection,*** response, ***or recovery***;

Or. en

Amendment 36
Evžen Tošenovský

Proposal for a regulation
Article 1 – paragraph 1 – point 2 – point b
Regulation (EU) 2019/881
Article 2 – point 14aa

Text proposed by the Commission	*Amendment*
	(14aa) ‘managed security service provider’ means managed a security service provider as defined in point (40) of Article 6 of Directive (EU) 2022/2555;

Or. en

Amendment 37
Ville Niinistö
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 1 – paragraph 1 – point 6
Regulation (EU) 2019/881
Article 47 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The Union rolling work programme shall in particular include a list of ICT products, ICT services and ICT processes	2. The Union rolling work programme shall in particular include a list of ICT products, ICT services and ICT processes

or categories thereof, and managed security services, that are capable of benefiting from being included in the scope of a European cybersecurity certification scheme.	or categories thereof, and managed security services, that are capable of benefiting from being included in the scope of a European cybersecurity certification scheme. ***Support measures to asses the needs for skilled employees, types of skills, existing training paths must be included along with measures to bridge any identified gaps.***

Or. en

Justification

The exercise to identify the ICT products, ICT services and ICT processes or categories thereof and managed security services must be accompanied by a skills assessment and measures to bridge the gaps.

Amendment 38
Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard

Proposal for a regulation
Article 1 – paragraph 1 – point 6
Regulation (EU) 2019/881
Article 47 – paragraph 3 – point a

Text proposed by the Commission	*Amendment*
(a) the availability and the development of national cybersecurity certification schemes covering a specific category of ICT products, ICT services, or ICT processes or managed security services and, in particular, as regards the risk of fragmentation;	(a) the availability and the development of national cybersecurity certification schemes ***and international and industry standards*** covering a specific category of ICT products, ICT services, or ICT processes or managed security services and, in particular, as regards the risk of fragmentation;

Or. en

Justification

The URWP should not only assess the development of national schemes, but also industry and international standards.

Amendment 39
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 1 – paragraph 1 – point 7
Regulation (EU) 2019/881
Article 49 – paragraph 7

Text proposed by the Commission	*Amendment*
(7) in Article 49, paragraph 7 is replaced by the following:	***deleted***
7. The Commission, based on the candidate scheme prepared by ENISA, may adopt implementing acts providing for a European cybersecurity certification scheme for ICT products, ICT services, ICT processes and managed security services which meets the requirements set out in Articles 51, 52 and 54. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 66(2).;	

Or. en

Amendment 40
Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard, Nicola Danti

Proposal for a regulation
Article 1 – paragraph 1 – point 7
Regulation (EU) 2019/881
Article 49 – paragraph 7

Text proposed by the Commission	*Amendment*
7. The Commission, based on the candidate scheme prepared by ENISA, may adopt ***implementing*** acts providing for a European cybersecurity certification scheme for ICT products, ICT services, ICT processes and managed security services which meets the requirements set out in Articles 51, 52 and 54. ***Those***	7. The Commission, based on the candidate scheme prepared by ENISA, may adopt ***delegated*** acts providing for a European cybersecurity certification scheme for ICT products, ICT services, ICT processes and managed security services which meets the requirements set out in Articles 51, 52 and 54.

implementing acts shall be adopted in accordance with the examination procedure referred to in Article 66(2).;

(This amendment applies throughout the text. Adopting it will necessitate corresponding changes throughout.)

Or. en

Justification

Since the adoption of the Cyber Security Act, no certification schemes have been adopted, nor has the Union Rolling Work Programme (URWP), which reflects wider stakeholder involvement, been formalized. Instead, some proposals, such as the EUCS, have introduced wide-ranging requirements that are not risk-based, hinder innovation and competitiveness, are highly political and therefore outside of ENISA's mandate in the CSA, and have not been properly consulted with relevant stakeholders or tested through impact assessments. It is therefore suggested that the adoption of a scheme is done through delegated act, and preceded by a impact assessment involving SCCG and ECCG consultations to improve the transparency of schemes and the effectiveness of the certification framework in general.

Amendment 41
Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard, Nicola Danti

Proposal for a regulation
Article 1 – paragraph 1 – point 7
Regulation (EU) 2019/881
Article 49 – paragraph 7a (new)

Text proposed by the Commission	*Amendment*
	7 a. Prior to adopting such delegated acts, the Commission, in cooperation with ENISA, shall carry out and publish an impact assessment of the proposed European cybersecurity certiciation scheme. While preparing the impact assessment, the Commission shall carry out public consultations and consultations with the SCCG and ECCG.

Or. en

Justification

Since the adoption of the Cyber Security Act, no certification schemes have been adopted, nor

has the Union Rolling Work Programme (URWP), which reflects wider stakeholder involvement, been formalized. Instead, some proposals, such as the EUCS, have introduced wide-ranging requirements that are not risk-based, hinder innovation and competitiveness, are highly political and therefore outside of ENISA's mandate in the CSA, and have not been properly consulted with relevant stakeholders or tested through impact assessments. It is therefore suggested that the adoption of a scheme is done through delegated act, and preceded by a impact assessment involving SCCG and ECCG consultations to improve the transparency of schemes and the effectiveness of the certification framework in general.

Amendment 42
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 1 – paragraph 1 – point 7 a (new)
Regulation (EU) 2019/881
Article 49 – paragraph 7a (new)

Text proposed by the Commission	*Amendment*
	(7 a) the following paragraph is inserted:
	'7a. The Commission, based on the candidate scheme prepared by ENISA, may adopt delegated acts providing for a European cybersecurity certification scheme for managed security services which meets the requirements set out in Articles 51, 52, and 54. Those delegated acts shall be adopted in accordance with the procedure referred to in Article 66a.'

Or. en

Amendment 43
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 1 – paragraph 1 – point 9
Regulation (EU) 2019/881
Article 51a – paragraph 1 – point b

Text proposed by the Commission	*Amendment*
(b) ensure that the provider has appropriate internal procedures in place to ensure that the managed security services are provided at a very high level of quality at all times ;	(b) ensure that the provider has appropriate internal procedures in place to ensure that the managed security services are provided at a very high level of quality ***and reliability*** at all times ;

Or. en

Amendment 44
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 1 – paragraph 1 – point 9
Regulation (EU) 2019/881
Article 51a – paragraph 1 – point g

Text proposed by the Commission	*Amendment*
(g) ensure that the ICT products, ICT services and ICT processes [and the hardware] deployed in the provision of the managed security services are secure by default and by design, do not contain known vulnerabilities and include the latest security updates;;	(g) ensure that the ICT products, ICT services and ICT processes [and the hardware] deployed in the provision of the managed security services are secure by default and by design, ***are provided with up-to-date software and hardware,*** do not contain known vulnerabilities and include the latest security updates;;

Or. en

Amendment 45
Evžen Tošenovský

Proposal for a regulation
Article 1 – paragraph 1 – point 9
Regulation (EU) 2019/881
Article 51a – paragraph 1 – point g

Text proposed by the Commission	*Amendment*
(g) ensure that the ICT products, ICT services and ICT processes ***[and the***	(g) ensure that the ICT products, ICT services and ICT processes deployed in the

hardware] deployed in the provision of the managed security services are secure by default and by design, do not contain known vulnerabilities and include the latest security updates;;	provision of the managed security services are secure by default and by design, do not contain known vulnerabilities and include the latest security updates;;

Or. en

Amendment 46
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 1 – paragraph 1 – point 13 – point b – point ii – point aa
Regulation (EU) 2019/881
Article 56 – paragraph 3 – third subparagraph – point a

Text proposed by the Commission	*Amendment*
(a) take into account the impact of the measures on the manufacturers or providers of such ICT products, ICT services, ICT processes or managed security services and on the users in terms of the cost of those measures and the societal or economic benefits stemming from the anticipated enhanced level of security for the targeted ICT products, ICT services, ICT processes or managed security services***;***;	(a) take into account the impact of the measures on the manufacturers or providers of such ICT products, ICT services, ICT processes or managed security services and on the users in terms of the cost of those measures and the societal or economic benefits stemming from the anticipated enhanced level of security for the targeted ICT products, ICT services, ICT processes or managed security services***, , including SMEs. The Commission shall ensure that SMEs have access to appropriate financial support in the implementation of the measures through already existing Union programmes***;

Or. en

Amendment 47
Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard, Nicola Danti

Proposal for a regulation
Article 1 – paragraph 1 – point 14

Regulation (EU) 2019/881
Article 57 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Without prejudice to paragraph 3 of this Article, national cybersecurity certification schemes, and the related procedures for the ICT products, ICT services, ICT processes and managed security services that are covered by a European cybersecurity certification scheme shall cease to produce effects from the date established in the ***implementing act adopted pursuant to Article 49(7)***. National cybersecurity certification schemes and the related procedures for the ICT products, ICT services, ICT processes and managed security services that are not covered by a European cybersecurity certification scheme shall continue to exist.	1. Without prejudice to paragraph 3 of this Article, national cybersecurity certification schemes, and the related procedures for the ICT products, ICT services, ICT processes and managed security services that are covered by a European cybersecurity certification scheme shall cease to produce effects from the date established in the ***delegated act***. National cybersecurity certification schemes and the related procedures for the ICT products, ICT services, ICT processes and managed security services that are not covered by a European cybersecurity certification scheme shall continue to exist. *(This amendment applies throughout the text. Adopting it will necessitate corresponding changes throughout.)*

Or. en

Justification

This reflects the amendment in article 49.

Amendment 48
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 1 – paragraph 1 – point 16 a (new)
Regulation (EU) 2019/881
Article 66a (new)

Text proposed by the Commission	*Amendment*
	(16 a) The following Article is inserted: ***Article 66a (new)*** ***Exercise of the delegation***

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 49 (7a) shall be conferred on the Commission for a period of 5 years from … [date of entry into force of the basic legislative act or any other date set by the co-legislators]. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the 5 year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

3. The delegation of power referred to in Article 49 (7a) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Article 49 (7a) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before

the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by [two months] at the initiative of the European Parliament or of the Council.

Or. en

Amendment 49
Evžen Tošenovský

Proposal for a regulation
Article 1 – paragraph 1 – point 17 – introductory part
Regulation (EU)2019/881
Article 67

Text proposed by the Commission	*Amendment*
(17) in Article 67, paragraphs ***2 and 3*** are replaced by the following:	(17) in Article 67, paragraphs ***1, 2, 3 and 4*** are replaced by the following:

Or. en

Amendment 50
Evžen Tošenovský

Proposal for a regulation
Article 1 – paragraph 1 – point 17
Regulation (EU) 2019/881
Article 67 – paragraph 1

Text proposed by the Commission	*Amendment*
	1 By 28 June 2024, and every four years thereafter, the Commission shall evaluate the impact, effectiveness and efficiency of ENISA and of its working practices, the possible need to modify ENISA's mandate and the financial implications of any such modification. The evaluation shall take into account any feedback provided to ENISA in response to its activities. Where the Commission considers that the continued

operation of ENISA is no longer justified in light of the objectives, mandate and tasks assigned to it, the Commission may propose that this Regulation be amended with regard to the provisions related to ENISA.

Or. en

Amendment 51
Evžen Tošenovský

Proposal for a regulation
Article 1 – paragraph 1 – point 17
Regulation (EU) 2019/881
Article 67 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The evaluation shall also assess the impact, effectiveness and efficiency of the provisions of Title III of this Regulation with regard to the objectives of ensuring an adequate level of cybersecurity of ICT products, ICT services, ICT processes and managed security services in the Union and improving the functioning of the internal market.	2. The evaluation shall also assess the impact, effectiveness and efficiency of the provisions of Title III of this Regulation with regard to the objectives of ensuring an adequate level of cybersecurity of ICT products, ICT services, ICT processes and managed security services in the Union and improving the functioning of the internal market***, including assessment of the procedure and timelines leading to preparation and adoption of the first European cybersecurity certification schemes and how this procedure could be improved and accelerated for subsequent certification schemes***.

Or. en

Amendment 52
Evžen Tošenovský

Proposal for a regulation
Article 1 – paragraph 1 – point 17
Regulation (EU) 2019/881
Article 67 – paragraph 4

Text proposed by the Commission	*Amendment*
	4. By 28 June 2024, and every four years thereafter, the Commission shall transmit a report on the evaluation together with its conclusions to the European Parliament, to the Council and to the Management Board. The findings of that report shall be made public. The report shall be accompanied, where necessary, by a legislative proposal.

Or. en