



Council of the European Union  
General Secretariat

Brussels, 03 October 2023

---

**Interinstitutional files:**  
**2023/0108 (COD)**

---

WK 12391/2023 INIT

REDACTED DOCUMENT ACCESSIBLE TO THE  
PUBLIC (16.04.2025). ONLY MARGINAL PERSONAL  
DATA HAVE BEEN REDACTED.

**LIMITE**

**CYBER**

*This is a paper intended for a specific community of recipients. Handling and  
further distribution are under the sole responsibility of community members.*

## WORKING DOCUMENT

---

From:	General Secretariat of the Council
To:	Delegations
Subject:	Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services - Delegations' comments

---

Delegations will find in the Annex comments from the BE, CZ, DK, FR and PT delegations.

## Table of Contents

BELGIUM .....	2
CZECH REPUBLIC .....	6
DENMARK .....	7
FRANCE .....	9
PORTUGAL .....	15



## BELGIUM

	Amendment suggestions to the Presidency compromise proposal on 15 September (in bold and underlined)	Comments
New Recital (1a)	<u>(1a) Article 67 of Regulation (EU) 2019/881 tasks the Commission to evaluate, by 28 June 2024, the impact, effectiveness and efficiency of, among others, the certification provisions of that Regulation, with a view to improve the functioning of the internal market. The present Regulation shall not inhibit or otherwise limit this evaluation which should follow a thorough, transparent and efficient process.</u>	Belgium looks very much forward to the Review of the working of the CSA, required by June 2024. It is vital to us that this Review should constitute (or lead to) a <b>thorough, effective and transparent debate</b> , also with Member States.  The provision of Art. 1 (17) in the present Regulation adds that the evaluation foreseen in Art. 67 of the original CSA would also include the evaluation of the MSS certification aspects. Since June 2024 will be too early to evaluate this aspect, it should be underlined that this should not impede the evaluation process in general.
Recital (4) + (5)	(4) Certification of managed security services <b>providers</b> 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 <b>by these</b>	Belgium continues to hold that the proposed amendments can be improved by <b>allowing the creation of certification schemes not (just) of Managed Security Services, but (also) of their providers.</b>

	<p><b><u>providers</u></b>. In light of the criticality of the managed security services <b><u>and their providers</u></b> and the sensitivity of the data they process, certification could provide potential customers with important guidance and assurance about the trustworthiness of these services <b><u>and their providers</u></b>. European certification schemes for managed security services <b><u>providers</u></b> contribute to avoiding fragmentation of the single market. This Regulation therefore aims at enhancing the functioning of the internal market.</p> <p><i>Similar amendments would be needed in Recital (5) and relevant articles (see below)</i></p>	<p>It is clear from the text and context that the intent of this proposal is to be able to indicate the trustworthiness of managed security service <b><u>providers</u></b>. The Cyber Posture of 2022, the Cyber Defence Policy of May 2023 and the Cyber Solidarity Act also require certification of service <b><u>providers</u></b>. Recital 5, Art. 1(5) and the new Art. 51a in the CSA+ also refer to security criteria that transcend the service itself and focus on organisational aspects (such as personnel and internal procedures). Only certifying the service will be insufficient to achieve the desired objective. Moreover, as stated above, in the case of MSSPs, the security of the service and of the organisation itself are intrinsically interconnected.</p> <p>Therefore Belgium proposes that this regulation would allow a scheme for the provider itself (MSSP) rather than for the service only (MSS). Such a scope adjustment to the MSSP will also be clearer and more efficient for the market, and give a firmer legal basis to the conformity assessment bodies, and <b>could help providers with achieving the cybersecurity requirements of NIS2.</b></p> <p>Additionally, we support the Presidency's compromise proposal to place all mentions of the Cyber Reserve between brackets and to <b>await the negotiations on the Cyber Solidarity Act to</b></p>
--	---	--

		include this reference.
New Recital (5c)	<p><u>(5c) When adopting Implementing Acts pursuant to the by this Regulation amended Article 49(7) of Regulation (EU) 2019/881, which will establish a certification scheme for Managed Security Services Providers, the Commission shall fully take into account the requirements for MSSPs contained in the Implementing Act to be adopted under Article 21(5) of NIS2 Directive EU (2022/2555). MSSPs should not be subject to divergent cybersecurity requirements in the Union. The Implementing Act under the NIS2 Directive could in this sense serve as a basic level of cybersecurity requirements, on which (a) future MSSP certification scheme(s) can build additional levels of assurance.</u></p>	<p><b>An Implementing act on cybersecurity requirements</b> for digital infrastructure entities, including MSSPs, will be adopted pursuant to the NIS2 Directive by October 2024.</p> <p>In this respect it is important to emphasize that the NIS2 directive focusses on the protection of an organization where the current CSA+ proposal limits certification to the services themselves. This is no semantic difference, but a significant difference in approach. Moreover, for this type of provider, the security of the services is intrinsically linked to the security of the organisation itself. This will inevitably link the future certification requirements of the MSS to the NIS2 requirements of the MSSPs and <b>reenforces the proposal to extend the scope of CSA+ for MSS to MSSP</b> . MSSPs should not become subject to conflicting requirements under NIS2 or such an MSS scheme. <b>Any future MSS certification scheme should therefore take into account the Implementing Act on MSSPs.</b></p>
Art. 1 (2) (b) on inserting a	<p>(a) the following point is inserted:</p> <p><i>‘(14a) ‘managed security service’ means a service <b>provided by</b></i></p>	<p>Since MSSPs are included in the scope of the NIS2 Directive, it is of vital importance that potential MSS schemes are coherent</p>

point (14a)	<p><b><u>managed security service providers as defined in Article 6(40) of Directive (EU) 2022/2555 of the European Parliament and of the Council<sup>2</sup></u></b>, consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, including incident response, penetration testing, security audits, and consultancy <b><i>related to technical support</i></b>’;</p>	<p>with the NIS2 implementation process for MSSPs. Thereby it is necessary that the <b>definition of MSS used in the CSA+ be identical to the definition in NIS2.</b></p>
Art. 1 (1) and following	<p>(1) in Article 1(1), first subparagraph, point (b) is replaced by the following:</p> <p><i>‘(b) a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services, ICT processes, and managed security services <b>providers</b> in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union.’;</i></p> <p><b><i>And identical changes to all other points (2)-(17) of Art. 1.</i></b></p>	<p>See comments on recitals (4) &amp; (5)</p>

## CZECH REPUBLIC

[...]

- (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.

- (5a) **The definition of managed security services should be consistent with that of managed security service providers enshrined in Article 2(40) of Directive (EU) 2022/2555. It includes a non-exhaustive list of managed security services to illustrate the kind of services that could qualify for certification schemes. There may be separate European cybersecurity certification schemes for different managed security services. The European cybersecurity certificates issued in accordance with such schemes should refer to specific managed security services of a specific provider of these services.**

- (5b) **Since the objective of this Regulation cannot be sufficiently achieved by the Member States but can rather, by reason of its scale and effects, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.**

- (6) 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]

[...]

**Commented** [REDACTED] NIS 2 defines MSSP in Art. 6(40), please correct.

CZ appreciates inclusion of this recital into the compromise text.

## DENMARK

Denmark would like to thank the Presidency for this opportunity to provide written comments to the amendments of the CSA.

In general, we would kindly like to request that the standard format for indicating changes is used in the compromise texts.

We recommend altering the newly introduced definition of “*managed security services*”, as we do not find it appropriate to extend the scope of the CSA to non-ICT related “*managed security services*” Instead, we suggest the following amendment:

“(2) Article 2 is amended as follows:

(b) the following point is inserted:

*‘(14a) ‘managed security service’ means a service consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, which may include including incident response, and penetration testing, security audits, and consultancy related to technical support.’*”

If the article 14.a is maintained, it should be clarified that only audits and consultancy related to cyber security should be covered by the definition.

In article 46(2) we find that a new formulation is necessary, in order to avoid subjective criteria. We must assume that a new certification scheme with three assurance levels (basic, substantial and high) will be established and that the formulation thus will have to accommodate all three levels. The current formulation of “very high” will be confusing for level basic. We suggest the following amendment:

“(5) in Article 46, paragraphs 1 and 2 are replaced by the following:

*‘1. The European cybersecurity certification framework shall be established in order to improve the conditions for the functioning of the internal market by increasing the level of cybersecurity within the Union and enabling a harmonised approach at Union level to European cybersecurity certification schemes, with a view to creating a digital single market for ICT products, ICT services, ICT processes and managed security services.’;*

*2. The European cybersecurity certification framework shall provide for a mechanism to establish European cybersecurity certification schemes. It shall attest that the ICT products, ICT services and ICT processes that have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity or confidentiality of*



*stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, services and processes throughout their life cycle. In addition, it shall attest that managed security services that have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity and confidentiality of data, which are accessed, processed, stored or transmitted in relation to the provision of those services, and that those services are provided continuously with the requisite competence, expertise and experience by staff with a **sufficient and appropriate** ~~very high~~ level of relevant technical knowledge and professional integrity.’;*”

As previously mentioned, we do not find it appropriate to extend the scope of the CSA to non-ICT related “*managed security services*”. We therefore do not see the need to introduce a new article 51a, but would rather find it better to integrate the new article 51a in article 51 – and avoid the subjective criteria. If article 51a is maintained, we at least need a new formulation of the subjective criteria, which should either be clarified in article 51a or the recital. We suggest the following amendment:

“(9) The following Article is inserted:

*‘Article 51a*

*Security objectives of European cybersecurity certification schemes for managed security services*

*‘A European cybersecurity certification scheme for managed security services shall be designed to achieve, as applicable, at least the following security objectives:*

*(a) **ensure** that the managed security services are provided with the requisite competence, expertise and experience, including that the staff in charge of providing these services has **a sufficient and appropriate** ~~a very high~~ level of technical knowledge and competence in the specific field, sufficient and appropriate experience, and ~~the highest degree of~~ professional integrity;*

*(b) **ensure** that the provider has appropriate internal procedures in place to ensure that the managed security services are provided at a **sufficient and appropriate** ~~very high~~ level of quality at all times ;’*”

## FRANCE

[...]

Whereas:

- (1) Regulation (EU) 2019/881 of the European Parliament and of the Council<sup>1</sup> sets up a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union.

Managed security services, are services provided by managed security service providers as defined in Article 6(4) of Directive (EU) 2022/2555 of the European Parliament and the Council<sup>2</sup>, which ~~are services consisting~~ 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 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~~<sup>3</sup>. Pursuant to Recital 86 of that Directive, managed security service providers in areas such as incident response, penetration testing ~~detection~~, security audits and consultancy related to preparedness and related technical support, play a particularly important role in assisting entities in their efforts to prevent, detect, respond to or recover from incidents.

Pursuant to the establishment of the European Digital Identity Wallets under the Regulation (EU) 2019/881, the identity wallet may rely on remote on-boarding procedures, enabling the identification of a person that would require a high level of confidence. In this regards, remote identification services could fall within the scope of managed security services certification to ensure a harmonized and secure framework for such services at EU level.

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.

[...]

- (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

<sup>1</sup> 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) (OJ L 151, 7.6.2019, p. 15).

<sup>2</sup> 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).

<sup>3</sup> ~~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).~~

**Commented** FR : proposal in order to be consistent with the article on definitions. Proposal to deal with detection instead of penetration testing in order to keep it flexible. Also, in order to be consistent with the needs of European operators (such as training / benefiting from exercises), consultancy should also concern preparedness.

**Formatted:** Font: 12 pt, Not Italic, Font color: Auto

**Formatted:** Font: 12 pt, Not Italic, Font color: Auto

**Commented** FR suggests to include remote identification services within the scope of managed security services.

The objective is anticipate future needs for the market with regards to the implementation of the european digital identity wallet, envisioned under the regulation 2019/881.

The e-wallet rests on the digital identity, and the certification could provide confidence and trust for a secure use of the e-wallet.

If a prioritisation of services should be foreseen, it should not prevent the possibility to include within the scope of managed security services the 'remote identification of person'.

**Formatted:** Font: 16 pt, Check spelling and grammar

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.

(5a) The definition of managed security services should be consistent with that of managed security service providers enshrined in Article 2(40) of Directive (EU) 2022/2555. It includes a non-exhaustive list of managed security services to illustrate the kind of services that could qualify for certification schemes.

**Commented** FR: as the need of the European market will evolve, FR recommends to avoid limiting the scope to the services listed in the definitions and suggests to delete this part.

(5b) Since the objective of this Regulation cannot be sufficiently achieved by the Member States but can rather, by reason of its scale and effects, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(6) 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]

*HAVE ADOPTED THIS REGULATION:*

*Amendments to Regulation (EU) 2019/881*

Regulation (EU) 2019/881 is amended as follows:

(1) in Article 1(1), first subparagraph, point (b) is replaced by the following:

*‘(b) a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services, ICT processes, and managed security services in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union.’;*

(2) Article 2 is amended as follows:

(a) points 9, 10 and 11 are replaced by the following:

*‘(9) ‘European cybersecurity certification scheme’ means a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services, ICT processes, or managed security services;*

*‘(10) ‘national cybersecurity certification scheme’ means a comprehensive set of rules, technical requirements, standards and procedures developed and adopted by a national public authority and that apply to the certification or conformity assessment of ICT products, ICT services, ICT processes and managed security services falling under the scope of the specific scheme;*

*(11) ‘European cybersecurity certificate’ means a document issued by a relevant body, attesting that a given ICT product, ICT service, ICT process or managed*

*security service has been evaluated for compliance with specific security requirements laid down in a European cybersecurity certification scheme;';*

- (b) the following point is inserted:

*'(14a) 'managed security service' means a service consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, including incident response, detection, penetration testing, security audits and consultancy related to preparedness, technical support and remote identification services;*

- (c) points 20, 21 and 22 are replaced by the following:

*'(20) 'technical specifications' means a document that prescribes the technical requirements to be met by, or conformity assessment procedures relating to, an ICT product, ICT service, ICT process or managed security service;*


*'(21) 'assurance level' means a basis for confidence that an ICT product, ICT service, ICT process or managed security service meets the security requirements of a specific European cybersecurity certification scheme, and indicates the level at which an ICT product, ICT service, ICT process or managed security service has been evaluated but as such does not measure the security of the ICT product, ICT service, ICT process or managed security service concerned;*

*'(22) 'conformity self-assessment' means an action carried out by a manufacturer or provider of ICT products, ICT services, ~~or~~ ICT processes or managed security services, which evaluates whether those ICT products, ICT services, ICT processes or managed security services meet the requirements of a specific European cybersecurity certification scheme;';*

- (3) in Article 4, paragraph 6 is replaced by the following

*'6. ENISA shall promote the use of European cybersecurity certification, with a view to avoiding the fragmentation of the internal market. ENISA shall contribute to the establishment and maintenance of a European cybersecurity certification framework in accordance with Title III of this Regulation, with a view to increasing the transparency of the cybersecurity of ICT products, ICT services, ICT processes, and managed security services, thereby strengthening trust in the digital internal market and its competitiveness.';*

[...]

**Commented**  FR : please see comment on the provision 2.

PUBLIC

(7) ~~in~~ Article 49, paragraph 7 is amended as follows ~~replaced by the following~~:

(a) paragraph 1 and 2 are replaced by the following :

*'1. Following a request from the Commission pursuant to Article 48, ENISA shall prepare a candidate scheme which meets the requirements set out in Articles 51, 51a, 52 and 54.*

*2. Following a request from the ECCG pursuant to Article 48(2), ENISA may prepare a candidate scheme which meets the requirements set out in Articles 51, 51a, 52 and 54. If ENISA refuses such a request, it shall give reasons for its refusal. Any decision to refuse such a request shall be taken by the Management Board.*

*3. On the basis of recommendation issued by the ECCG, certification schemes should be prioritised.*

**'(b) paragraph 7 is replaced by the following :**

*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).';*

**Commented** [REDACTED] FR : as it will be quite challenging to develop/adopt/implement at once all schemes, FR suggests to prioritise certification services and the ECCG is the expertise body that should be entitled to assess such prioritisation

**Formatted:** Font: Not Bold

**Formatted:** Font: Not Bold

**Formatted:** Font: Not Bold

(8) Article 51 is amended as follows:

(a) the title is replaced by the following:

***Security objectives of European cybersecurity certification schemes for ICT products, ICT services and ICT processes***

(b) the introductory sentence is replaced by the following:

*'A European cybersecurity certification scheme for ICT products, ICT services or ICT processes shall be designed to achieve, as applicable, at least the following security objectives:'*

(9) The following Article is inserted:

***'Article 51a***

***Security objectives of European cybersecurity certification schemes for managed security services***



*'A European cybersecurity certification scheme for managed security services shall be designed to achieve, as applicable, at least the following security objectives:*

- (a) ~~ensure~~ that the managed security services are provided with the requisite competence, expertise and experience, including that the staff in charge of providing these services has a very high level of technical knowledge and competence in the specific field, sufficient and appropriate experience, and the highest degree of professional integrity;*
- (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 ;*
- (c) to protect data accessed, stored, transmitted or otherwise processed in relation to the provision of managed security services against accidental or unauthorised access, storage, disclosure, destruction, other processing, or loss or alteration or lack of availability;*
- (d) ~~ensure~~ that the availability and access to data, services and functions is restored in a timely manner in the event of a physical or technical incident;*
- (e) ~~ensure~~ that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;*
- (f) to record, and enable to assess, which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;*
- (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;';*

Article 51(b)

Formatted: Font: Bold, Italic

National security concerns

Formatted: Centered

Security objectives of European cybersecurity certification schemes for managed security services should not exclude the possibility for national competent authority to add up national security objectives when it concerns security and defense national interest.

Formatted: Font: Bold, Italic

Formatted: Font color: Auto

Formatted: Font color: Auto

**Commented** FR suggests to include this sentence as national security objectives fall within the competence of Member states.

Formatted: Font: Italic

[...]

## PORTUGAL

Portugal welcomes the proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services, flagging it as an opportunity not to be missed. In that sense Portugal stresses the need to widen the scope of the amendment at the risk of losing this opportunity for years to come.

Due to the infrastructural nature of managed services, the amendment should provide for the European certification of these types of services, and not only managed security services.

Additionally, Portugal also sees a need for European certification schemes directed at the cybersecurity management systems of entities, to assess their compliance with the uptake of appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

This would enable the implementation of certification schemes for SMEs, which already exist in different forms throughout the EU, but also of schemes targeted for entities within the scope of NIS 2, supporting its effective implementation by defining baseline cybersecurity standards applicable across the Union.

Moreover, it would allow the creation of European cybersecurity-specific management systems certifications, since there seems to be a market gap in this area as well as risk of fragmentation due to the emergence of national schemes.

The amendment enabling this type of certification is required since cybersecurity management systems rely on the implementation of organisational procedures and on active human intervention, and assessing their level of technical and specific competences, expertise and experience is not currently foreseen in the CSA.

A new category of minimum-security objectives should be developed for the entities' cybersecurity, in line with the NIS 2 provisions.

This would also enable the development of sector-specific cybersecurity management systems certification schemes, which, due to their being tailored to those sectors, would better address their cybersecurity needs, could further boost cybersecurity in vital sectors for the society and economy and would contribute to a common European minimum cybersecurity level in such crucial sectors.

In short, by enabling both above stated certifications, namely managed services and entities' cybersecurity-specific management systems,

- the quality of managed services entities under the NIS 2 scope would be improved and their comparability increased;

- complementarity of the CSA with the NIS 2 Directive would be reinforced and the European certification schemes could contribute to the implementation of NIS 2 security objectives;
- fragmentation of the internal market could be avoided, since there seems to be a concrete risk of fragmentation of the internal market in this domain;
- cybersecurity certification could be used by National Competent Authorities, supporting their activities in the implementation of the NIS 2 Directive.

Even if it could be actively promoted by Cybersecurity National Competent Authorities, certification of services and of cybersecurity-specific management systems should and would remain voluntary and not compulsory, so as not to restrict access to the market.

In line with this view, Portugal suggests the following amendments:

Article 1(1), first subparagraph, point (b):

*‘(b) a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services, ICT processes, ~~and~~ managed ~~security~~ services and entities’ cybersecurity management systems in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union.’*

Article 2, points 9, 10 and 11:

*‘(9) ‘European cybersecurity certification scheme’ means a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services, ICT processes, ~~or~~ managed ~~security~~ services and entities’ cybersecurity management systems;*

*‘(10) ‘national cybersecurity certification scheme’ means a comprehensive set of rules, technical requirements, standards and procedures developed and adopted by a national public authority and that apply to the certification or conformity assessment of ICT products, ICT services, ICT processes, ~~and~~ managed ~~security~~ services and entities’ cybersecurity management systems falling under the scope of the specific scheme;*

*(11) ‘European cybersecurity certificate’ means a document issued by a relevant body, attesting that a given ICT product, ICT service, ICT process, ~~or~~ managed ~~security~~ service or entity’s cybersecurity management systems has been evaluated for compliance with specific security requirements laid down in a European cybersecurity certification scheme;’*

with other relevant articles and recitals being amended accordingly.