Council of the European Union

Brussels, 20 November 2023
(OR. en)

15652/23

Interinstitutional File: 2023/0108(COD)

CYBER 295
JAI 1515
TELECOM 341
DATAPROTECT 322
MI 1004
IND 612
CODEC 2192

NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	14136/23
No. Cion doc.:	8511/23
Subject:	Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services - 4-column table

Delegations will find in the Annex a table concerning the above legislative proposal, which contains:

- the Commission proposal of 18 April 2023,

- amendments adopted by the European Parliament on 25 October 2023, and

- the Council's mandate approved on 15 November 2023.

ANNEX

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2019/881 as regards managed security services (Text with EEA relevance)

2023/0108(COD)

DRAFT [DRAFT - EP and Council mandates 17.11.2023]

	Commission Proposal	EP Mandate	Council Mandate
Formula			
1	2023/0108 (COD)	2023/0108 (COD)	2023/0108 (COD)
Proposal Title			
2	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2019/881 as regards managed security services (Text with EEA relevance)	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2019/881 as regards managed security services (Text with EEA relevance)	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2019/881 as regards managed security services (Text with EEA relevance)
Formula			
3	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Citation 1			
4	Having regard to the Treaty on the Functioning of the European Union, and in particular Article	Having regard to the Treaty on the Functioning of the European Union, and in particular Article	Having regard to the Treaty on the Functioning of the European Union, and in particular Article

	Commission Proposal	EP Mandate	Council Mandate
	114 thereof,	114 thereof,	114 thereof,
Citation 2			
5	Having regard to the proposal from the European Commission,	Having regard to the proposal from the European Commission,	Having regard to the proposal from the European Commission,
Citation 3			
6	After transmission of the draft legislative act to the national parliaments,	After transmission of the draft legislative act to the national parliaments,	After transmission of the draft legislative act to the national parliaments,
Citation 4			
7	Having regard to the opinion of the European Economic and Social Committee,	Having regard to the opinion of the European Economic and Social Committee,	Having regard to the opinion of the European Economic and Social Committee,
Citation 5			
8	Having regard to the opinion of the Committee of the Regions;	Having regard to the opinion of the Committee of the Regions;	Having regard to the opinion of the Committee of the Regions;
Citation 6			
9	Acting in accordance with the ordinary legislative procedure,	Acting in accordance with the ordinary legislative procedure,	Acting in accordance with the ordinary legislative procedure,
Formula			

	Commission Proposal	EP Mandate	Council Mandate
10	Whereas:	Whereas:	Whereas:
Recital 1			
11	(1) Regulation (EU) 2019/881 of the European Parliament and of the Council[1] 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. _____ 1. 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).	(1) Regulation (EU) 2019/881 of the European Parliament and of the Council[1] sets up a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ***information and communications technology (ICT)*** ~~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. _____ 1. ***[1]*** 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).	(1) Regulation (EU) 2019/881 of the European Parliament and of the Council[1] 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. _____ 1. 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).
Recital 1a			
11a		***(1a) In order to ensure the Union's resilience***	

	Commission Proposal	EP Mandate	Council Mandate
		to cyberattacks and to prevent any vulnerabilities in the Union market, this Regulation is intended to complement the horizontal regulatory framework establishing comprehensive cybersecurity requirements for all products with digital elements in accordance with Regulation (EU) .../... of the European Parliament and of the Council[1] (2022/0272(COD)), by setting up essential requirements for cybersecurity managed services, their application and their trustworthiness. ***1. [1] Regulation (EU) .../... of the European Parliament and of the Council of ... on ... (OJ L, …, ELI: …).***	
Recital 2			
12	(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[1]. Pursuant to Recital 86 of that Directive, managed security service providers in areas	(2) Managed security services, which are services consisting of carrying out, or providing assistance for, activities relating to their customers' cybersecurity risk management, ***including detection, response to or recovery from incidents,*** have gained increasing importance in the prevention and mitigation of cybersecurity incidents. ***The activities of the providers of managed security services consist of services relating to prevention, identification, protection, detection, analysis, containment, response and recovery, including, but not limited to, cyber threat***	(2) Managed security services **are services provided by managed security service providers as defined in Article 6, point (40), of Directive (EU) 2022/2555 of the European Parliament and of the Council[1], which consist**~~, 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

	Commission Proposal	EP Mandate	Council Mandate
	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. _____ 1. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).	***intelligence provision, real time threat monitoring through proactive techniques, including security-by-design, risk assessment, extended detection, remediation and response.*** 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[1]. 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. _____ 1. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p.	belonging to a sector of high criticality pursuant to Directive (EU) 2022/2555 ~~of the European Parliament and of the Council~~[12]. 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. _____ 1. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80). **2. 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**

	Commission Proposal	EP Mandate	Council Mandate
		80).	**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).**
Recital 3			
13	(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 strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats	(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 strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats	(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 strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats

	Commission Proposal	EP Mandate	Council Mandate
	and incidents] correspond to 'managed security services' in accordance with this Regulation.	and incidents] correspond to 'managed security services' in accordance with this Regulation.	and incidents] correspond to 'managed security services' in accordance with this Regulation.]
Recital 4			
14	(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.	(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.
Recital 4a			
14a		***(4a) European certification schemes for managed security services should lead to the uptake of those services and to increased competition in the field, taking into account the specific needs of both providers and beneficiaries. Those schemes should, therefore, strike a balance between the their objective and the potential regulatory, administrative and financial burden that***	

	Commission Proposal	EP Mandate	Council Mandate
		providers, especially microenterprises or small and medium-sized enterprises (SMEs), could encounter. Additionally, the schemes should encourage the use of certified managed security services by contributing to the accessibility thereof, especially for smaller actors, such as microenterprises and SMEs, as well as local and regional authorities which have limited capacity and resources, but which are more prone to cybersecurity breaches with financial, legal, reputational, and operational implications.	
Recital 4b			
14b		***(4b) 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 Digital Decade Policy Programme, especially with regard to the goal that 75% of Union undertakings start using Cloud, AI or Big Data, that more than 90% of microenterprises and SMEs reach at least a basic level of digital intensity and that key public services are offered online.***	
Recital 4c			
14c		***(4c) In the current fast evolving digital and technological landscape, the offer of***	

	Commission Proposal	EP Mandate	Council Mandate
		educational resources and formal trainings differ and knowledge can be acquired in various ways, both formal, for example through university or courses and non-formal, for example through on the job trainings or longstanding work experience in the relevant field.	
Recital 5			
15	(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 ***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*~~***development of certification schemes established pursuant to this*** Regulation ~~*(EU) 2018/1725 of the European Parliament and*~~***should take into account the results and recommendations*** of the ~~*Council and delivered an opinion on [DD/MM/YYYY*~~***evaluation and review provided***	(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

	Commission Proposal	EP Mandate	Council Mandate
		for in this Regulation.	
Recital 5a			
15a		***(5a) With a view to facilitating the growth of a reliable Union market, whilst also creating partnerships with likeminded third countries, including in light of the provisions of the Regulation (EU) .../... of the European Parliament and of the Council[1] (2023/0109(COD)) with regard to the access to the EU Cybersecurity Reserve, the certification process established within the framework established by this Regulation should be streamlined to ensure international recognition and alignment with international standards.*** ***1. Regulation (EU) .../... of the European Parliament and of the Council of ... on ...(OJ L, …, ELI: …).***	
Recital 5b			
15b		***(5b) With the aim of ensuring the development of a trustworthy Union market for managed security services, the providers thereof and Member States should collaborate and contribute to the collection of data on the situation and the evolution of the cybersecurity labour market.***	

	Commission Proposal	EP Mandate	Council Mandate
Recital 5c			
15c		***(5c) A Union-wide coordinated approach to strengthening the resilience of critical infrastructure is based on the Member States' capacity building. However, the Union is faced with a talent gap, characterised 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. Therefore, in order to facilitate the emergence of high-quality, essential managed security services and to have a better overview of the composition of the Union cybersecurity workforce, cooperation between Member States, the Commission, ENISA and stakeholders, including the private sector and academia, should be strengthened through 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 as well as the integration of cybersecurity knowledge and training in educational programmes, while ensuring access to apprenticeships and traineeships for young people, including persons living in***	

	Commission Proposal	EP Mandate	Council Mandate
		disadvantaged regions, such as islands, sparsely populated, rural and remote areas. Those measures should also aim to attract more women and girls in the field and contribute towards addressing the gender gap in science, technology, engineering, and mathematics. The private sector should also aim to deliver on-the-job training addressing the most in-demand skills, involving public administration and start-ups, as well as microenterprises and SMEs.	
Recital 5d			
15d		***(5d) Appropriate funding and resources should be ensured for the purpose of the additional tasks entrusted to ENISA by the amendments to Regulation (EU) 2019/881 introduced by this Regulation.***	
Recital 5e			
15e		***(5e) In order to supplement certain non-essential elements of this Regulation, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission to provide for a European cybersecurity certification scheme for ICT products, ICT services, ICT processes and managed security services. It is of particular importance that the Commission carry out***	

	Commission Proposal	EP Mandate	Council Mandate
		appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[1] . In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts. ***1. OJ L 123, 12.5.2016, p. 1***	
Recital 5a			
15f			**(5a) The definition of managed security services should be consistent with that of managed security service providers enshrined in Article 6, point (40), of Directive (EU) 2022/2555. It includes a non-exhaustive list of managed security services that could qualify for certification schemes. Managed security service means a service consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, such as incident detection or response, penetration testing, security audits, and consultancy related to technical support. Managed security services could encompass**

	Commission Proposal	EP Mandate	Council Mandate
			cybersecurity services that support the preparedness, prevention and mitigation of, and recovery from, cybersecurity incidents. 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.
Recital 5b			
15g			**(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.**
Recital 6			
15h		***(5e) 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***	**(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**

	Commission Proposal	EP Mandate	Council Mandate
		delivered an opinion on [DD/MM/YYYY][2] ***2. OJ c.../...***	**and delivered an opinion on [DD/MM/YYYY],**
Formula			
16	HAVE ADOPTED THIS REGULATION:	HAVE ADOPTED THIS REGULATION:	HAVE ADOPTED THIS REGULATION:
Article 1			
17	Article 1 Amendments to Regulation (EU) 2019/881	Article 1 Amendments to Regulation (EU) 2019/881	Article 1 Amendments to Regulation (EU) 2019/881
Article 1, first paragraph			
18	Regulation (EU) 2019/881 is amended as follows:	Regulation (EU) 2019/881 is amended as follows:	Regulation (EU) 2019/881 is amended as follows:
Article 1, first paragraph, point (1)			
19	(1) in Article 1(1), first subparagraph, point (b) is replaced by the following:	(1) in Article 1(1), first subparagraph, point (b) is replaced by the following:	(1) in Article 1(1), first subparagraph, point (b) is replaced by the following:
Article 1, first paragraph, point (1), amending provision, numbered paragraph (b)			
20	‘ (b) a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of	‘ (b) a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of	‘ (b) a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of

	Commission Proposal	EP Mandate	Council Mandate
	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.; ,	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.; ,	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.; ,
Article 1, first paragraph, point (2)			
21	(2) Article 2 is amended as follows:	(2) Article 2 is amended as follows:	(2) Article 2 is amended as follows:
Article 1, first paragraph, point (2)(a)			
22	(a) points 9, 10 and 11 are replaced by the following:	(a) points 9, 10 and 11 are replaced by the following:	(a) points 9, 10 and 11 are replaced by the following:
Article 1, first paragraph, point (2)(a), amending provision, numbered paragraph (9)			
23	‘ (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;	‘ (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;	‘ (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;
Article 1, first paragraph, point (2)(a), amending provision, numbered paragraph (10)			

	Commission Proposal	EP Mandate	Council Mandate
24	(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;	(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;	(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;
Article 1, first paragraph, point (2)(a), amending provision, numbered paragraph (11)			
25	(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;; '	(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;***'***; '	(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;; '
Article 1, first paragraph, point (2)(b)			
26	(b) the following point is inserted:	(b) the following point is inserted:	(b) the following point is inserted:
Article 1, first paragraph, point (2)(b), amending provision, numbered paragraph (14a)			
27	' (14a) 'managed security service' means a service consisting of carrying out, or providing	' (14a) 'managed security service' means a service ***provided to a third party*** consisting of	' (14a) 'managed security service' means a service consisting of carrying out, or providing

	Commission Proposal	EP Mandate	Council Mandate
	assistance for, activities relating to cybersecurity risk management, including incident response, penetration testing, security audits and consultancy; '	carrying out, or providing assistance for, ***or advice on*** activities relating to cybersecurity risk management, including incident ~~*response,*~~ ***handling,*** penetration testing, security audits and ~~*consultancy*~~***consulting'***; '	assistance for, activities relating to cybersecurity risk management, ~~including~~**such as** incident **detection or** response, penetration testing, security audits**,** and consultancy **related to technical support'**; '
Article 1, first paragraph, point (2)(c)			
28	(c) points 20, 21 and 22 are replaced by the following:	(c) points 20, 21 and 22 are replaced by the following:	(c) points 20, 21 and 22 are replaced by the following:
Article 1, first paragraph, point (2)(c), amending provision, numbered paragraph (20)			
29	' (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;	' (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;	' (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;
Article 1, first paragraph, point (2)(c), amending provision, numbered paragraph (21)			
30	(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	(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	(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

	Commission Proposal	EP Mandate	Council Mandate
	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;	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;	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;
Article 1, first paragraph, point (2)(c), amending provision, numbered paragraph (22)			
31	(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;; '	(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;; '	(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;; '
Article 1, first paragraph, point (3)			
32	(3) in Article 4, paragraph 6 is replaced by the following	(3) in Article 4, paragraph 6 is replaced by the following	(3) in Article 4, paragraph 6 is replaced by the following
Article 1, first paragraph, point (3), amending provision, numbered paragraph (6)			
33	' 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	' 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	' 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

	Commission Proposal	EP Mandate	Council Mandate
	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.; ,	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.; ,	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.; ,
Article 1, first paragraph, point (4)			
34	(4) Article 8 is amended as follows:	(4) Article 8 is amended as follows:	(4) Article 8 is amended as follows:
Article 1, first paragraph, point (4)(a)			
35	(a) paragraph 1 is replaced by the following:	(a) paragraph 1 is replaced by the following:	(a) paragraph 1 is replaced by the following:
Article 1, first paragraph, point (4)(a), amending provision, numbered paragraph (1)			
36	‘ 1. ENISA shall support and promote the development and implementation of Union policy on cybersecurity certification of ICT products, ICT services, ICT processes and managed security services, as established in Title III of this Regulation, by:	‘ 1. ENISA shall support and promote the development and implementation of Union policy on cybersecurity certification of ICT products, ICT services, ICT processes and managed security services, as established in Title III of this Regulation, by:	‘ 1. ENISA shall support and promote the development and implementation of Union policy on cybersecurity certification of ICT products, ICT services, ICT processes and managed security services, as established in Title III of this Regulation, by:
Article 1, first paragraph, point (4)(a), amending provision, numbered paragraph (1), point (a)			
37	(a) monitoring developments, on an ongoing basis, in related areas of standardisation and	(a) monitoring developments, on an ongoing basis, in related areas of standardisation and	(a) monitoring developments, on an ongoing basis, in related areas of standardisation and

	Commission Proposal	EP Mandate	Council Mandate
	recommending appropriate technical specifications for use in the development of European cybersecurity certification schemes pursuant to Article 54(1), point (c), where standards are not available;	recommending appropriate technical specifications for use in the development of European cybersecurity certification schemes pursuant to Article 54(1), point (c), where standards are not available;	recommending appropriate technical specifications for use in the development of European cybersecurity certification schemes pursuant to Article 54(1), point (c), where standards are not available;
Article 1, first paragraph, point (4)(a), amending provision, numbered paragraph (1), point (b)			
38	(b) preparing candidate European cybersecurity certification schemes ('candidate schemes') for ICT products, ICT services, ICT processes and managed security services in accordance with Article 49;	(b) preparing candidate European cybersecurity certification schemes ('candidate schemes') for ICT products, ICT services, ICT processes and managed security services in accordance with Article 49;	(b) preparing candidate European cybersecurity certification schemes ('candidate schemes') for ICT products, ICT services, ICT processes and managed security services in accordance with Article 49;
Article 1, first paragraph, point (4)(a), amending provision, numbered paragraph (1), point (c)			
39	(c) evaluating adopted European cybersecurity certification schemes in accordance with Article 49(8);	(c) evaluating adopted European cybersecurity certification schemes in accordance with Article 49(8);	(c) evaluating adopted European cybersecurity certification schemes in accordance with Article 49(8);
Article 1, first paragraph, point (4)(a), amending provision, numbered paragraph (1), point (d)			
40	(d) participating in peer reviews pursuant to Article 59(4);	(d) participating in peer reviews pursuant to Article 59(4);	(d) participating in peer reviews pursuant to Article 59(4);
Article 1, first paragraph, point (4)(a), amending provision, numbered paragraph (1), point (e)			
41	(e) assisting the Commission in providing the secretariat of the ECCG pursuant to Article 62(5).;	(e) assisting the Commission in providing the secretariat of the ECCG pursuant to Article 62(5).;	(e) assisting the Commission in providing the secretariat of the ECCG pursuant to Article 62(5).;

	Commission Proposal	EP Mandate	Council Mandate
	’	’	’
Article 1, first paragraph, point (4)(b)			
42	(b) paragraph 3 is replaced by the following:	(b) paragraph 3 is replaced by the following:	(b) paragraph 3 is replaced by the following:
Article 1, first paragraph, point (4)(b), amending provision, numbered paragraph (3)			
43	‘ 3. ENISA shall compile and publish guidelines and develop good practices, concerning the cybersecurity requirements for ICT products, ICT services, ICT processes and managed security services, in cooperation with national cybersecurity certification authorities and industry in a formal, structured and transparent way.; ’	‘ 3. ENISA shall compile and publish guidelines and develop good practices, concerning the cybersecurity requirements for ICT products, ICT services, ICT processes and managed security services, in cooperation with national cybersecurity certification authorities and industry in a formal, structured and transparent way.; ’	‘ 3. ENISA shall compile and publish guidelines and develop good practices, concerning the cybersecurity requirements for ICT products, ICT services, ICT processes and managed security services, in cooperation with national cybersecurity certification authorities and industry in a formal, structured and transparent way.; ’
Article 1, first paragraph, point (4)(c)			
44	(c) paragraph 5 is replaced by the following:	(c) paragraph 5 is replaced by the following:	(c) paragraph 5 is replaced by the following:
Article 1, first paragraph, point (4)(c), amending provision, numbered paragraph (5)			
45	‘ 5. ENISA shall facilitate the establishment and take-up of European and international standards for risk management and for the security of ICT products, ICT services, ICT processes and	‘ 5. ENISA shall facilitate the establishment and take-up of European and international standards for risk management and for the security of ICT products, ICT services, ICT processes and	‘ 5. ENISA shall facilitate the establishment and take-up of European and international standards for risk management and for the security of ICT products, ICT services, ICT processes and

	Commission Proposal	EP Mandate	Council Mandate
	managed security services.; ’	managed security services.; ’	managed security services.; ’
Article 1, first paragraph, point (5)			
46	(5) in Article 46, paragraphs 1 and 2 are replaced by the following:	(5) in Article 46, paragraphs 1 and 2 are replaced by the following:	(5) in Article 46, paragraphs 1 and 2 are replaced by the following:
Article 1, first paragraph, point (5), amending provision, numbered paragraph (1)			
47	‘ 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.’;	‘ 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.’;	‘ 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.’;
Article 1, first paragraph, point (5), amending provision, numbered paragraph (2)			
48	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	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	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

	Commission Proposal	EP Mandate	Council Mandate
	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 very high level of relevant technical knowledge and professional integrity.; ’	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 very high level of relevant technical knowledge and professional integrity.; ’	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 ~~very high~~ **sufficient and appropriate** level of relevant technical knowledge and professional integrity.**’**; ’
Article 1, first paragraph, point (6)			
49	(6) in Article 47, paragraphs 2 and 3 are replaced by the following:	(6) in Article 47, paragraphs 2 and 3 are replaced by the following:	(6) in Article 47, paragraphs 2 and 3 are replaced by the following:
Article 1, first paragraph, point (6), amending provision, numbered paragraph (2)			
50	‘ 2. The Union rolling work programme shall in particular include a list of ICT products, ICT services and ICT processes or categories	‘ 2. The Union rolling work programme shall in particular include a list of ICT products, ICT services and ICT processes or categories	‘ 2. The Union rolling work programme shall in particular include a list of ICT products, ICT services and ICT processes or categories

	Commission Proposal	EP Mandate	Council Mandate
	thereof, and managed security services, that are capable of benefiting from being included in the scope of a European cybersecurity certification scheme.	thereof, and managed security services, that are capable of benefiting from being included in the scope of a European cybersecurity certification scheme***. In that context, the Commission may include an in-depth assessment of existing training paths to bridge identified skills gaps and a list of proposals for addressing the needs for skilled employees and types of skills***.	thereof, and managed security services, that are capable of benefiting from being included in the scope of a European cybersecurity certification scheme.
Article 1, first paragraph, point (6), amending provision, numbered paragraph (3)			
51	3. Inclusion of specific ICT products, ICT services and ICT processes or categories thereof, or of managed security services, in the Union rolling work programme shall be justified on the basis of one or more of the following grounds:	3. Inclusion of specific ICT products, ICT services and ICT processes or categories thereof, or of managed security services, in the Union rolling work programme shall be justified on the basis of one or more of the following grounds:	3. Inclusion of specific ICT products, ICT services and ICT processes or categories thereof, or of managed security services, in the Union rolling work programme shall be justified on the basis of one or more of the following grounds:
Article 1, first paragraph, point (6), amending provision, numbered paragraph (3), point (a)			
52	(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 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 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;
Article 1, first paragraph, point (6), amending provision, numbered paragraph (3), point (b)			
53	(b) relevant Union or Member State law or policy;	(b) relevant Union or Member State law or policy;	(b) relevant Union or Member State law or policy;

	Commission Proposal	EP Mandate	Council Mandate
Article 1, first paragraph, point (6), amending provision, numbered paragraph (3), point (c)			
54	(c) market demand;	(c) market demand;	(c) market demand;
Article 1, first paragraph, point (6), amending provision, numbered paragraph (3), point (ca)			
54a		***(ca) technological developments and the availability and development of international cybersecurity certification schemes and international and industrial standards.***	
Article 1, first paragraph, point (6), amending provision, numbered paragraph (3), point (d)			
55	(d) developments in the cyber threat landscape;	(d) developments in the cyber threat landscape;	(d) developments in the cyber threat landscape;
Article 1, first paragraph, point (6), amending provision, numbered paragraph (3), point (e)			
56	(e) request for the preparation of a specific candidate scheme by the ECCG.;	(e) request for the preparation of a specific candidate scheme by the ECCG.;	(e) request for the preparation of a specific candidate scheme by the ECCG.;
Article 1, first paragraph, point (7)			
57	(7) in Article 49, paragraph 7 is replaced by the following:	(7) ~~*in*~~ Article 49, ~~*paragraph 7 is replaced by the following:*~~***is amended as follows:***	(7) ~~in~~ Article 49~~, paragraph 7 is replaced by the following~~ **is amended as follows:,**
Article 1, first paragraph, point (7), first subparagraph			

	Commission Proposal	EP Mandate	Council Mandate
57a			**(a) paragraphs 1 and 2 are replaced by the following:**
Article 1, first paragraph, point (7), fist subparagraph, amending provision, first paragraph			
57b			‘ **1. Following a request from the Commission pursuant to Article 48, ENISA shall prepare a candidate scheme which meets the applicable requirements set out in Articles 51, 51a, 52 and 54.**
Article 1, first paragraph, point (7), first subparagraph, amending provision, second paragraph			
57c			**2. Following a request from the ECCG pursuant to Article 48(2), ENISA may prepare a candidate scheme which meets the applicable 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.’;** ’
Article 1, first paragraph, point (7), second subparagraph			
57d		***(a) paragraph 7 is replaced by the following:***	**(b) paragraph 7 is replaced by the following:**
Article 1, first paragraph, point (6a), third subparagraph, point (a)			

	Commission Proposal	EP Mandate	Council Mandate
57e			
Article 1, first paragraph, point (6a), third subparagraph, point (a), amending provision, numbered paragraph (7)			
58	‘ 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).; ’	‘ 7. ~~–~~***‘7.*** The Commission, based on the candidate scheme prepared by ENISA, ~~*may*~~***is empowered to*** adopt ***delegated acts in accordance with Article 65a, supplementing this Regulation by*** ~~*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).*~~***’***;	‘ 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, **51a,** 52 and 54. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 66(2).**’**; ’
(b) the following paragraph is inserted			
58a		***(b) the following paragraph is inserted:***	
Article 1, first paragraph, point (7a), amending provision, numbered paragraph (7a)			
58b		***7a. ‘Before adopting such delegated acts, the Commission, in cooperation with ENISA, shall carry out and publish an impact assessment of the proposed European cybersecurity certification scheme. While preparing the impact assessment, the Commission shall carry***	

	Commission Proposal	EP Mandate	Council Mandate
		out public consultations and shall consult the SCCG and ECCG.'; ,	
Article 1, first paragraph, point (8)			
59	(8) Article 51 is amended as follows:	(8) Article 51 is amended as follows:	(8) Article 51 is amended as follows:
Article 1, first paragraph, point (8)(a)			
60	(a) the title is replaced by the following:	(a) the title is replaced by the following:	(a) the title is replaced by the following:
Article 1, first paragraph, point (8)(a), amending provision, first subparagraph			
61	‘ Security objectives of European cybersecurity certification schemes for ICT products, ICT services and ICT processes ,	‘ ‘Security objectives of European cybersecurity certification schemes for ICT products, ICT services and ICT processes-’ ,	‘ Security objectives of European cybersecurity certification schemes for ICT products, ICT services and ICT processes ,
Article 1, first paragraph, point (8)(b)			
62	(b) the introductory sentence is replaced by the following:	(b) the introductory sentence is replaced by the following:	(b) the introductory sentence is replaced by the following:
Article 1, first paragraph, point (8)(b), amending provision, first paragraph			
63	‘ A European cybersecurity certification scheme	‘ A European cybersecurity certification scheme	‘ A European cybersecurity certification scheme

	Commission Proposal	EP Mandate	Council Mandate
	for ICT products, ICT services or ICT processes shall be designed to achieve, as applicable, at least the following security objectives: ; ,	for ICT products, ICT services or ICT processes shall be designed to achieve, as applicable, at least the following security objectives: ; ,	for ICT products, ICT services or ICT processes shall be designed to achieve, as applicable, at least the following security objectives: ; ,
Article 1, first paragraph, point (9)			
64	(9) The following Article is inserted:	(9) The following Article is inserted:	(9) The following Article is inserted:
Article 1, first paragraph, point (9), amending provision, first paragraph			
65	‘ Article 51a	‘ Article 51a	‘ Article 51a
Article 1, first paragraph, point (9), amending provision, second paragraph			
66	Security objectives of European cybersecurity certification schemes for managed security services	Security objectives of European cybersecurity certification schemes for managed security services	Security objectives of European cybersecurity certification schemes for managed security services
Article 1, first paragraph, point (9), amending provision, third paragraph			
67	‘A European cybersecurity certification scheme for managed security services shall be designed to achieve, as applicable, at least the following security objectives:	‘A European cybersecurity certification scheme for managed security services shall be designed to achieve, as applicable, at least the following security objectives:	‘A European cybersecurity certification scheme for managed security services shall be designed to achieve, as applicable, at least the following security objectives:
Article 1, first paragraph, point (9), amending provision, third paragraph, point (a)			
68			

	Commission Proposal	EP Mandate	Council Mandate
	(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;	(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;	(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~~ **sufficient and appropriate** level of technical knowledge and competence in the specific field, sufficient and appropriate experience, and the highest degree of professional integrity;
Article 1, first paragraph, point (9), amending provision, third paragraph, point (b)			
69	(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 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~~ **sufficient and appropriate** level of quality at all times ;
Article 1, first paragraph, point (9), amending provision, third paragraph, point (c)			
70	(c) 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;	(c) 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;	(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;
Article 1, first paragraph, point (9), amending provision, third paragraph, point (d)			
71	(d) ensure that the availability and access to data, services and functions is restored in a	(d) ensure that the availability and access to data, services and functions is restored in a	(d) ~~ensure~~ that the availability and access to data, services and functions is restored in a

	Commission Proposal	EP Mandate	Council Mandate
	timely manner in the event of a physical or technical incident;	timely manner in the event of a physical or technical incident;	timely manner in the event of a physical or technical incident;
Article 1, first paragraph, point (9), amending provision, third paragraph, point (e)			
72	(e) ensure that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;	(e) ensure that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;	(e) ~~ensure~~ that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;
Article 1, first paragraph, point (9), amending provision, third paragraph, point (f)			
73	(f) record, and enable to assess, which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;	(f) record, and enable to assess, which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;	(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;
Article 1, first paragraph, point (9), amending provision, third paragraph, point (g)			
74	(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 ***and are provided with up-to-date software and hardware***, ~~-~~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~~,~~**;** **- the ICT products deployed in the provision of the managed security services** do not contain known **exploitable** vulnerabilities and include the latest security updates;**'**; ,
Article 1, first paragraph, point (10)			

	Commission Proposal	EP Mandate	Council Mandate
75	(10) Article 52 is amended as follows:	(10) Article 52 is amended as follows:	(10) Article 52 is amended as follows:
Article 1, first paragraph, point (10)(a)			
76	(a) paragraph 1 is replaced by the following:	(a) paragraph 1 is replaced by the following:	(a) paragraph 1 is replaced by the following:
Article 1, first paragraph, point (10)(a), amending provision, numbered paragraph (1)			
77	‘ 1. A European cybersecurity certification scheme may specify one or more of the following assurance levels for ICT products, ICT services, ICT processes and managed security services: ‘basic’, ‘substantial’ or ‘high’. The assurance level shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service, ICT process or managed security service, in terms of the probability and impact of an incident.; ’	‘ 1. A European cybersecurity certification scheme may specify one or more of the following assurance levels for ICT products, ICT services, ICT processes and managed security services: ‘basic’, ‘substantial’ or ‘high’. The assurance level shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service, ICT process or managed security service, in terms of the probability and impact of an incident.; ’	‘ 1. A European cybersecurity certification scheme may specify one or more of the following assurance levels for ICT products, ICT services, ICT processes and managed security services: ‘basic’, ‘substantial’ or ‘high’. The assurance level shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service, ICT process or managed security service, in terms of the probability and impact of an incident.; ’
Article 1, first paragraph, point (10)(b)			
78	(b) paragraph 3 is replaced by the following:	(b) paragraph 3 is replaced by the following:	(b) paragraph 3 is replaced by the following:
Article 1, first paragraph, point (10)(b), amending provision, numbered paragraph (3)			
79	‘ 3. The security requirements corresponding to	‘ 3. The security requirements corresponding to	‘ 3. The security requirements corresponding to

	Commission Proposal	EP Mandate	Council Mandate
	each assurance level shall be provided in the relevant European cybersecurity certification scheme, including the corresponding security functionalities and the corresponding rigour and depth of the evaluation that the ICT product, ICT service, ICT process or managed security service is to undergo.; ’	each assurance level shall be provided in the relevant European cybersecurity certification scheme, including the corresponding security functionalities and the corresponding rigour and depth of the evaluation that the ICT product, ICT service, ICT process or managed security service is to undergo.; ’	each assurance level shall be provided in the relevant European cybersecurity certification scheme, including the corresponding security functionalities and the corresponding rigour and depth of the evaluation that the ICT product, ICT service, ICT process or managed security service is to undergo.; ’
Article 1, first paragraph, point (10)(c)			
80	(c) paragraphs 5, 6 and 7 are replaced by the following:	(c) paragraphs 5, 6 and 7 are replaced by the following:	(c) paragraphs 5, 6 and 7 are replaced by the following:
Article 1, first paragraph, point (10)(c), amending provision, numbered paragraph (5)			
81	‘ 5. A European cybersecurity certificate or EU statement of conformity that refers to assurance level ‘basic’ shall provide assurance that the ICT products, ICT services, ICT processes and managed security services for which that certificate or that EU statement of conformity is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known basic risks of incidents and cyberattacks. The evaluation activities to be undertaken shall include at least a review of technical documentation. Where such a review is not appropriate, substitute evaluation activities with equivalent effect shall	‘ 5. A European cybersecurity certificate or EU statement of conformity that refers to assurance level ‘basic’ shall provide assurance that the ICT products, ICT services, ICT processes and managed security services for which that certificate or that EU statement of conformity is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known basic risks of incidents and cyberattacks. The evaluation activities to be undertaken shall include at least a review of technical documentation. Where such a review is not appropriate, substitute evaluation activities with equivalent effect shall	‘ 5. A European cybersecurity certificate or EU statement of conformity that refers to assurance level ‘basic’ shall provide assurance that the ICT products, ICT services, ICT processes and managed security services for which that certificate or that EU statement of conformity is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known basic risks of incidents and cyberattacks. The evaluation activities to be undertaken shall include at least a review of technical documentation. Where such a review is not appropriate, substitute evaluation activities with equivalent effect shall

	Commission Proposal	EP Mandate	Council Mandate
	be undertaken.	be undertaken.	be undertaken.
Article 1, first paragraph, point (10)(c), amending provision, numbered paragraph (6)			
82	6. A European cybersecurity certificate that refers to assurance level ‘substantial’ shall provide assurance that the ICT products, ICT services, ICT processes and managed security services for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the ICT products, ICT services, ICT processes or managed security services correctly implement the necessary security functionalities. Where any such evaluation activities are not appropriate, substitute evaluation activities with equivalent effect shall be undertaken.	6. A European cybersecurity certificate that refers to assurance level ‘substantial’ shall provide assurance that the ICT products, ICT services, ICT processes and managed security services for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the ICT products, ICT services, ICT processes or managed security services correctly implement the necessary security functionalities. Where any such evaluation activities are not appropriate, substitute evaluation activities with equivalent effect shall be undertaken.	6. A European cybersecurity certificate that refers to assurance level ‘substantial’ shall provide assurance that the ICT products, ICT services, ICT processes and managed security services for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the ICT products, ICT services, ICT processes or managed security services correctly implement the necessary security functionalities. Where any such evaluation activities are not appropriate, substitute evaluation activities with equivalent effect shall be undertaken.
Article 1, first paragraph, point (10)(c), amending provision, numbered paragraph (7)			
83	7. A European cybersecurity certificate that refers to assurance level ‘high’ shall provide assurance that the ICT products, ICT services,	7. A European cybersecurity certificate that refers to assurance level ‘high’ shall provide assurance that the ICT products, ICT services,	7. A European cybersecurity certificate that refers to assurance level ‘high’ shall provide assurance that the ICT products, ICT services,

	Commission Proposal	EP Mandate	Council Mandate
	ICT processes and managed security services for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities; testing to demonstrate that the ICT products, ICT services, ICT processes or managed security services correctly implement the necessary security functionalities at the state of the art; and an assessment of their resistance to skilled attackers, using penetration testing. Where any such evaluation activities are not appropriate, substitute activities with equivalent effect shall be undertaken.; ’	ICT processes and managed security services for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities; testing to demonstrate that the ICT products, ICT services, ICT processes or managed security services correctly implement the necessary security functionalities at the state of the art; and an assessment of their resistance to skilled attackers, using penetration testing. Where any such evaluation activities are not appropriate, substitute activities with equivalent effect shall be undertaken.; ’	ICT processes and managed security services for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities; testing to demonstrate that the ICT products, ICT services, ICT processes or managed security services correctly implement the necessary security functionalities at the state of the art; and an assessment of their resistance to skilled attackers, using penetration testing. Where any such evaluation activities are not appropriate, substitute activities with equivalent effect shall be undertaken.; ’
Article 1, first paragraph, point (11)			
84	(11) in Article 53, paragraphs 1, 2 and 3 are replaced by the following:	(11) in Article 53, paragraphs 1, 2 and 3 are replaced by the following:	(11) in Article 53, paragraphs 1, 2 and 3 are replaced by the following:
Article 1, first paragraph, point (11), amending provision, numbered paragraph (1)			
85	‘ 1. A European cybersecurity certification scheme may allow for the conformity self-assessment under the sole responsibility of the	‘ 1. A European cybersecurity certification scheme may allow for the conformity self-assessment under the sole responsibility of the	‘ 1. A European cybersecurity certification scheme may allow for the conformity self-assessment under the sole responsibility of the

	Commission Proposal	EP Mandate	Council Mandate
	manufacturer or provider of ICT products, ICT services, ICT processes or managed security services. Conformity self-assessment shall be permitted only in relation to ICT products, ICT services, ICT processes and managed security services that present a low risk corresponding to assurance level 'basic'.	manufacturer or provider of ICT products, ICT services, ICT processes or managed security services. Conformity self-assessment shall be permitted only in relation to ICT products, ICT services, ICT processes and managed security services that present a low risk corresponding to assurance level 'basic'.	manufacturer or provider of ICT products, ICT services, ICT processes or managed security services. Conformity self-assessment shall be permitted only in relation to ICT products, ICT services, ICT processes and managed security services that present a low risk corresponding to assurance level 'basic'.
Article 1, first paragraph, point (11), amending provision, numbered paragraph (2)			
86	2. The manufacturer or provider of ICT products, ICT services, ICT processes or managed security services may issue an EU statement of conformity stating that the fulfilment of the requirements set out in the scheme has been demonstrated. By issuing such a statement, the manufacturer or provider of ICT products, ICT services, ICT processes or managed security services shall assume responsibility for the compliance of the ICT product, ICT service, ICT process or managed security service with the requirements set out in that scheme.	2. The manufacturer or provider of ICT products, ICT services, ICT processes or managed security services may issue an EU statement of conformity stating that the fulfilment of the requirements set out in the scheme has been demonstrated. By issuing such a statement, the manufacturer or provider of ICT products, ICT services, ICT processes or managed security services shall assume responsibility for the compliance of the ICT product, ICT service, ICT process or managed security service with the requirements set out in that scheme.	2. The manufacturer or provider of ICT products, ICT services, ICT processes or managed security services may issue an EU statement of conformity stating that the fulfilment of the requirements set out in the scheme has been demonstrated. By issuing such a statement, the manufacturer or provider of ICT products, ICT services, ICT processes or managed security services shall assume responsibility for the compliance of the ICT product, ICT service, ICT process or managed security service with the requirements set out in that scheme.
Article 1, first paragraph, point (11), amending provision, numbered paragraph (3)			
87	3. The manufacturer or provider of ICT products, ICT services, ICT processes or managed security services shall make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity of the	3. The manufacturer or provider of ICT products, ICT services, ICT processes or managed security services shall make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity of the	3. The manufacturer or provider of ICT products, ICT services, ICT processes or managed security services shall make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity of the

	Commission Proposal	EP Mandate	Council Mandate
	ICT products, ICT services or managed security services with the scheme available to the national cybersecurity certification authority referred to in Article 58 for the period provided for in the corresponding European cybersecurity certification scheme. A copy of the EU statement of conformity shall be submitted to the national cybersecurity certification authority and to ENISA.; ’	ICT products, ICT services or managed security services with the scheme available to the national cybersecurity certification authority referred to in Article 58 for the period provided for in the corresponding European cybersecurity certification scheme. A copy of the EU statement of conformity shall be submitted to the national cybersecurity certification authority and to ENISA.; ’	ICT products, ICT services or managed security services with the scheme available to the national cybersecurity certification authority referred to in Article 58 for the period provided for in the corresponding European cybersecurity certification scheme. A copy of the EU statement of conformity shall be submitted to the national cybersecurity certification authority and to ENISA.; ’
Article 1, first paragraph, point (12)			
88	(12) in Article 54, paragraph 1 is amended as follows:	(12) in Article 54, paragraph 1 is amended as follows:	(12) in Article 54, paragraph 1 is amended as follows:
Article 1, first paragraph, point (12)(a)			
89	(a) point (a) is replaced by the following:	(a) point (a) is replaced by the following:	(a) point (a) is replaced by the following:
Article 1, first paragraph, point (12)(aa)			
89a			*deleted*
Article 1, first paragraph, point (12)(aa), amending provision, numbered paragraph (a)			
90	‘ *(a)* the subject matter and scope of the certification scheme, including the type or	‘ (a) the subject matter and scope of the certification scheme, including the type or	‘ (a) the subject matter and scope of the certification scheme, including the type or

	Commission Proposal	EP Mandate	Council Mandate
	categories of ICT products, ICT services, ICT processes and managed security services covered;; ,	categories of ICT products, ICT services, ICT processes and managed security services covered;; ,	categories of ICT products, ICT services, ICT processes and managed security services covered;; ,
Article 1, first paragraph, point (12)(ab)			
90a			**(aa) point (g) is replaced by the following:**
Article 1, first paragraph, point (12)(ab), amending provision, first paragraph			
90b			‘ **‘(g) the specific evaluation criteria and methods to be used, including types of evaluation, in order to demonstrate that the applicable security objectives referred to in Articles 51 and 51a are achieved;’;** ,
Article 1, first paragraph, point (12)(b)			
91	(b) point (j) is replaced by the following:	(b) point (j) is replaced by the following:	(b) point (j) is replaced by the following:
Article 1, first paragraph, point (12)(b), amending provision, numbered paragraph (j)			
92	‘ (j) rules for monitoring compliance of ICT products, ICT services, ICT processes and managed security services with the requirements of the European cybersecurity	‘ (j) rules for monitoring compliance of ICT products, ICT services, ICT processes and managed security services with the requirements of the European cybersecurity	‘ (j) rules for monitoring compliance of ICT products, ICT services, ICT processes and managed security services with the requirements of the European cybersecurity

	Commission Proposal	EP Mandate	Council Mandate
	certificates or the EU statements of conformity, including mechanisms to demonstrate continued compliance with the specified cybersecurity requirements;; ,	certificates or the EU statements of conformity, including mechanisms to demonstrate continued compliance with the specified cybersecurity requirements;; ,	certificates or the EU statements of conformity, including mechanisms to demonstrate continued compliance with the specified cybersecurity requirements;; ,
Article 1, first paragraph, point (12)(c)			
93	(c) point (l) is replaced by the following:	(c) point (l) is replaced by the following:	(c) point (l) is replaced by the following:
Article 1, first paragraph, point (12)(c), amending provision, numbered paragraph (l)			
94	‘ (l) rules concerning the consequences for ICT products, ICT services, ICT processes and managed security services that have been certified or for which an EU statement of conformity has been issued, but which do not comply with the requirements of the scheme;; ,	‘ (l) rules concerning the consequences for ICT products, ICT services, ICT processes and managed security services that have been certified or for which an EU statement of conformity has been issued, but which do not comply with the requirements of the scheme;; ,	‘ (l) rules concerning the consequences for ICT products, ICT services, ICT processes and managed security services that have been certified or for which an EU statement of conformity has been issued, but which do not comply with the requirements of the scheme;; ,
Article 1, first paragraph, point (12)(d)			
95	(d) point (o) is replaced by the following:	(d) point (o) is replaced by the following:	(d) point (o) is replaced by the following:
Article 1, first paragraph, point (12)(d), amending provision, numbered paragraph (o)			
96	‘ (o) the identification of national or international cybersecurity certification	‘ (o) the identification of national or international cybersecurity certification	‘ (o) the identification of national or international cybersecurity certification

	Commission Proposal	EP Mandate	Council Mandate
	schemes covering the same type or categories of ICT products, ICT services, ICT processes and managed security services, security requirements, evaluation criteria and methods, and assurance levels;; ,	schemes covering the same type or categories of ICT products, ICT services, ICT processes and managed security services, security requirements, evaluation criteria and methods, and assurance levels;; ,	schemes covering the same type or categories of ICT products, ICT services, ICT processes and managed security services, security requirements, evaluation criteria and methods, and assurance levels;; ,
Article 1, first paragraph, point (12)(e)			
97	(e) point (q) is replaced by the following:	(e) point (q) is replaced by the following:	(e) point (q) is replaced by the following:
Article 1, first paragraph, point (12)(e), amending provision, numbered paragraph (q)			
98	‘ (q) the period of the availability of the EU statement of conformity, technical documentation, and all other relevant information to be made available by the manufacturer or provider of ICT products, ICT services, ICT or managed security services processes;; ,	‘ (q) the period of the availability of the EU statement of conformity, technical documentation, and all other relevant information to be made available by the manufacturer or provider of ICT products, ICT services, ICT or managed security services processes;; ,	‘ (q) the period of the availability of the EU statement of conformity, technical documentation, and all other relevant information to be made available by the manufacturer or provider of ICT products, ICT services, ICT **processes** or managed security services ~~processes~~;**’**; ,
Article 1, first paragraph, point (13)			
99	(13) Article 56 is amended as follows:	(13) Article 56 is amended as follows:	(13) Article 56 is amended as follows:
Article 1, first paragraph, point (13)(a)			
100	(a) paragraph 1 is replaced by the following:	(a) paragraph 1 is replaced by the following:	(a) paragraph 1 is replaced by the following:

	Commission Proposal	EP Mandate	Council Mandate
Article 1, first paragraph, point (13)(a), amending provision, numbered paragraph (1)			
101	‘ 1. ICT products, ICT services, ICT processes and managed security services that have been certified under a European cybersecurity certification scheme adopted pursuant to Article 49 shall be presumed to comply with the requirements of such scheme ’	‘ 1. ICT products, ICT services, ICT processes and managed security services that have been certified under a European cybersecurity certification scheme adopted pursuant to Article 49 shall be presumed to comply with the requirements of such scheme ’	‘ 1. ICT products, ICT services, ICT processes and managed security services that have been certified under a European cybersecurity certification scheme adopted pursuant to Article 49 shall be presumed to comply with the requirements of such scheme ’
Article 1, first paragraph, point (13)(b)			
102	(b) paragraph 3 is amended as follows:	(b) paragraph 3 is amended as follows:	(b) paragraph 3 is amended as follows:
Article 1, first paragraph, point (13)(b)(i)			
103	(i) the first subparagraph is replaced by the following:	(i) the first subparagraph is replaced by the following:	(i) the first subparagraph is replaced by the following:
Article 1, first paragraph, point (13)(b)(i), amending provision, first paragraph			
104	‘ The Commission shall regularly assess the efficiency and use of the adopted European cybersecurity certification schemes and whether a specific European cybersecurity certification scheme is to be made mandatory through relevant Union law to ensure an adequate level	‘ The Commission shall regularly assess the efficiency and use of the adopted European cybersecurity certification schemes and whether a specific European cybersecurity certification scheme is to be made mandatory through relevant Union law to ensure an adequate level	‘ The Commission shall regularly assess the efficiency and use of the adopted European cybersecurity certification schemes and whether a specific European cybersecurity certification scheme is to be made mandatory through relevant Union law to ensure an adequate level

	Commission Proposal	EP Mandate	Council Mandate
	of cybersecurity of ICT products, ICT services, ICT processes and managed security services in the Union and improve the functioning of the internal market. The first such assessment shall be carried out by 31 December 2023, and subsequent assessments shall be carried out at least every two years thereafter. Based on the outcome of those assessments, the Commission shall identify the ICT products, ICT services, ICT processes and managed security services covered by an existing certification scheme which are to be covered by a mandatory certification scheme.; ’	of cybersecurity of ICT products, ICT services, ICT processes and managed security services in the Union and improve the functioning of the internal market. The first such assessment shall be carried out by 31 December 2023, and subsequent assessments shall be carried out at least every two years thereafter. Based on the outcome of those assessments, the Commission shall identify the ICT products, ICT services, ICT processes and managed security services covered by an existing certification scheme which are to be covered by a mandatory certification scheme.; ’	of cybersecurity of ICT products, ICT services, ICT processes and managed security services in the Union and improve the functioning of the internal market. The first such assessment shall be carried out by 31 December 2023, and subsequent assessments shall be carried out at least every two years thereafter. Based on the outcome of those assessments, the Commission shall identify the ICT products, ICT services, ICT processes and managed security services covered by an existing certification scheme which are to be covered by a mandatory certification scheme.; ’
Article 1, first paragraph, point (13)(b)(ii)			
105	(ii) the third subparagraph is amended as follows:	(ii) the third subparagraph is amended as follows:	(ii) the third subparagraph is amended as follows:
Article 1, first paragraph, point (13)(b)(ii)(aa)			
106	(aa) point (a) is replaced by the following:	(aa) point (a) is replaced by the following:	(aa) point (a) is replaced by the following:
Article 1, first paragraph, point (13)(b)(ii)(aa), amending provision, numbered paragraph (a)			
107	‘ (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	‘ (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	‘ (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

	Commission Proposal	EP Mandate	Council Mandate
	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;; ,	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;; ,	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;; ,
Article 1, first paragraph, point (13)(b)(ii)(bb)			
108	(bb) point (d) is replaced by the following:	(bb) point (d) is replaced by the following:	(bb) point (d) is replaced by the following:
Article 1, first paragraph, point (13)(b)(ii)(bb), amending provision, numbered paragraph (d)			
109	‘ (d) take into account any implementation deadlines, transitional measures and periods, in particular with regard to the possible impact of the measure on the manufacturers or providers of ICT products, ICT services, ICT processes or managed security services, including SMEs;; ,	‘ (d) take into account any implementation deadlines, transitional measures and periods, in particular with regard to the possible impact of the measure on the manufacturers or providers of ICT products, ICT services, ICT processes or managed security services, including ***the specific interests and needs of microenterprises and SMEs;’*** ~~*SMEs;*~~; ,	‘ (d) take into account any implementation deadlines, transitional measures and periods, in particular with regard to the possible impact of the measure on the manufacturers or providers of ICT products, ICT services, ICT processes or managed security services, including SMEs;; ,
Article 1, first paragraph, point (13)(b)(iia)			
109a		***(iii) the following subparagraph is added:***	
Article 1, first paragraph, point (13)(b)(iia), amending provision, first paragraph			
109b			

	Commission Proposal	EP Mandate	Council Mandate
		‘ ***‘With regard to the third subparagraph, point (d) of this Article, the Commission shall ensure appropriate financial support in the regulatory framework of existing Union programmes, in particular in order to ease the financial burden on microenterprises and SMEs, including start-ups acting in the field of managed security services.’;*** ’	
Article 1, first paragraph, point (13)(c)			
110	(c) paragraphs 7 and 8 are replaced by the following:	(c) paragraphs 7 and 8 are replaced by the following:	(c) paragraphs 7 and 8 are replaced by the following:
Article 1, first paragraph, point (13)(c), amending provision, numbered paragraph (7)			
111	‘ 7. The natural or legal person who submits ICT products, ICT services, ICT processes or managed security services for certification shall make available to the national cybersecurity certification authority referred to in Article 58, where that authority is the body issuing the European cybersecurity certificate, or to the conformity assessment body referred to in Article 60 all information necessary to conduct the certification.	‘ 7. The natural or legal person who submits ICT products, ICT services, ICT processes or managed security services for certification shall make available to the national cybersecurity certification authority referred to in Article 58, where that authority is the body issuing the European cybersecurity certificate, or to the conformity assessment body referred to in Article 60 all information necessary to conduct the certification.	‘ 7. The natural or legal person who submits ICT products, ICT services, ICT processes or managed security services for certification shall make available to the national cybersecurity certification authority referred to in Article 58, where that authority is the body issuing the European cybersecurity certificate, or to the conformity assessment body referred to in Article 60 all information necessary to conduct the certification.
Article 1, first paragraph, point (13)(c), amending provision, numbered paragraph (8)			

	Commission Proposal	EP Mandate	Council Mandate
112	8. The holder of a European cybersecurity certificate shall inform the authority or body referred to in paragraph 7 of any subsequently detected vulnerabilities or irregularities concerning the security of the certified ICT product, ICT service, ICT process or managed security services that may have an impact on its compliance with the requirements related to the certification. That authority or body shall forward that information without undue delay to the national cybersecurity certification authority concerned. ’	8. The holder of a European cybersecurity certificate shall inform the authority or body referred to in paragraph 7 of any subsequently detected vulnerabilities or irregularities concerning the security of the certified ICT product, ICT service, ICT process or managed security services that may have an impact on its compliance with the requirements related to the certification. That authority or body shall forward that information without undue delay to the national cybersecurity certification authority concerned. ’	8. The holder of a European cybersecurity certificate shall inform the authority or body referred to in paragraph 7 of any subsequently detected vulnerabilities or irregularities concerning the security of the certified ICT product, ICT service, ICT process or managed security services that may have an impact on its compliance with the requirements related to the certification. That authority or body shall forward that information without undue delay to the national cybersecurity certification authority concerned. ’
Article 1, first paragraph, point (14)			
113	(14) in Article 57, paragraphs 1 and 2 are replaced by the following:	(14) in Article 57, paragraphs 1 and 2 are replaced by the following:	(14) in Article 57, paragraphs 1 and 2 are replaced by the following:
Article 1, first paragraph, point (14), amending provision, numbered paragraph (1)			
114	‘ 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	‘ 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*** ~~implementing~~ act adopted pursuant to Article 49(7). National	‘ 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

	Commission Proposal	EP Mandate	Council Mandate
	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.	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.	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.
Article 1, first paragraph, point (14), amending provision, numbered paragraph (2)			
115	2. Member States shall not introduce new national cybersecurity certification schemes for ICT products, ICT services, ICT processes and managed security services already covered by a European cybersecurity certification scheme that is in force.; ,	2. Member States shall not introduce new national cybersecurity certification schemes for ICT products, ICT services, ICT processes and managed security services already covered by a European cybersecurity certification scheme that is in force.; ,	2. Member States shall not introduce new national cybersecurity certification schemes for ICT products, ICT services, ICT processes and managed security services already covered by a European cybersecurity certification scheme that is in force.; ,
Article 1, first paragraph, point (15)			
116	(15) Article 58 is amended as follows:	(15) Article 58 is amended as follows:	(15) Article 58 is amended as follows:
Article 1, first paragraph, point (15)(a)			
117	(a) paragraph 7 is amended as follows:	(a) paragraph 7 is amended as follows:	(a) paragraph 7 is amended as follows:
Article 1, first paragraph, point (15)(a)(i)			
118	(i) points (a) and (b) are replaced by the following:	(i) points (a) and (b) are replaced by the following:	(i) points (a) and (b) are replaced by the following:

	Commission Proposal	EP Mandate	Council Mandate
Article 1, first paragraph, point (15)(a)(i), amending provision, numbered paragraph (a)			
119	‘ (a) supervise and enforce rules included in European cybersecurity certification schemes pursuant to point (j) of Article 54(1) for the monitoring of the compliance of ICT products, ICT services, ICT processes and managed security services with the requirements of the European cybersecurity certificates that have been issued in their respective territories, in cooperation with other relevant market surveillance authorities;	‘ (a) supervise and enforce rules included in European cybersecurity certification schemes pursuant to point (j) of Article 54(1) for the monitoring of the compliance of ICT products, ICT services, ICT processes and managed security services with the requirements of the European cybersecurity certificates that have been issued in their respective territories, in cooperation with other relevant market surveillance authorities;	‘ (a) supervise and enforce rules included in European cybersecurity certification schemes pursuant to point (j) of Article 54(1) for the monitoring of the compliance of ICT products, ICT services, ICT processes and managed security services with the requirements of the European cybersecurity certificates that have been issued in their respective territories, in cooperation with other relevant market surveillance authorities;
Article 1, first paragraph, point (15)(a)(i), amending provision, numbered paragraph (b)			
120	(b) monitor compliance with and enforce the obligations of the manufacturers or providers of ICT products, ICT services, ICT processes or managed security services that are established in their respective territories and that carry out conformity self-assessment, and shall, in particular, monitor compliance with and enforce the obligations of such manufacturers or providers set out in Article 53(2) and (3) and in the corresponding European cybersecurity certification scheme;; ’	(b) monitor compliance with and enforce the obligations of the manufacturers or providers of ICT products, ICT services, ICT processes or managed security services that are established in their respective territories and that carry out conformity self-assessment, and shall, in particular, monitor compliance with and enforce the obligations of such manufacturers or providers set out in Article 53(2) and (3) and in the corresponding European cybersecurity certification scheme;; ’	(b) monitor compliance with and enforce the obligations of the manufacturers or providers of ICT products, ICT services, ICT processes or managed security services that are established in their respective territories and that carry out conformity self-assessment, and shall, in particular, monitor compliance with and enforce the obligations of such manufacturers or providers set out in Article 53(2) and (3) and in the corresponding European cybersecurity certification scheme;; ’
Article 1, first paragraph, point (15)(a)(ii)			
121			

	Commission Proposal	EP Mandate	Council Mandate
	(ii) point (h) is replaced by the following:	(ii) point (h) is replaced by the following:	(ii) point (h) is replaced by the following:
Article 1, first paragraph, point (15)(a)(ii), amending provision, numbered paragraph (h)			
122	‘ (h) cooperate with other national cybersecurity certification authorities or other public authorities, including by sharing information on the possible non-compliance of ICT products, ICT services, ICT processes and managed security services with the requirements of this Regulation or with the requirements of specific European cybersecurity certification schemes; and; ’	‘ (h) cooperate with other national cybersecurity certification authorities or other public authorities, including by sharing information on the possible non-compliance of ICT products, ICT services, ICT processes and managed security services with the requirements of this Regulation or with the requirements of specific European cybersecurity certification schemes; and; ’	‘ (h) cooperate with other national cybersecurity certification authorities or other public authorities, including by sharing information on the possible non-compliance of ICT products, ICT services, ICT processes and managed security services with the requirements of this Regulation or with the requirements of specific European cybersecurity certification schemes; and; ’
Article 1, first paragraph, point (15)(b)			
123	(b) paragraph 9 is replaced by the following:	(b) paragraph 9 is replaced by the following:	(b) paragraph 9 is replaced by the following:
Article 1, first paragraph, point (15)(b), amending provision, numbered paragraph (9)			
124	‘ 9. National cybersecurity certification authorities shall cooperate with each other and with the Commission, in particular, by exchanging information, experience and good practices as regards cybersecurity certification and technical issues concerning the cybersecurity of ICT products, ICT services, ICT and managed security services processes.;	‘ 9. National cybersecurity certification authorities shall cooperate with each other and with the Commission, in particular, by exchanging information, experience and good practices as regards cybersecurity certification and technical issues concerning the cybersecurity of ICT products, ICT services, ICT and managed security services processes.;	‘ 9. –National cybersecurity certification authorities shall cooperate with each other and with the Commission, in particular, by exchanging information, experience and good practices as regards cybersecurity certification and technical issues concerning the cybersecurity of ICT products, ICT services, ICT **processes** and managed security services

	Commission Proposal	EP Mandate	Council Mandate
	’	’	~~processes~~.’; ’
Article 1, first paragraph, point (16)			
125	(16) in Article 59 (3), points (b) and (c) are replaced by the following:	(16) in Article 59 (3), points (b) and (c) are replaced by the following:	(16) in Article 59 (3), points (b) and (c) are replaced by the following:
Article 1, first paragraph, point (16a)			
125a		This line will be deleted by the technical service of TTE.	
Article 1, first paragraph, point (16), amending provision, numbered paragraph (b)			
126	‘ (b) the procedures for supervising and enforcing the rules for monitoring the compliance of ICT products, ICT services, ICT processes and managed security services with European cybersecurity certificates pursuant to Article 58(7), point (a);	‘ (b) the procedures for supervising and enforcing the rules for monitoring the compliance of ICT products, ICT services, ICT processes and managed security services with European cybersecurity certificates pursuant to Article 58(7), point (a);	‘ (b) the procedures for supervising and enforcing the rules for monitoring the compliance of ICT products, ICT services, ICT processes and managed security services with European cybersecurity certificates pursuant to Article 58(7), point (a);
Article 1, first paragraph, point (16), amending provision, numbered paragraph (c)			
127	(c) the procedures for monitoring and enforcing the obligations of manufacturers or providers of ICT products, ICT services, ICT processes or managed security services pursuant to Article	(c) the procedures for monitoring and enforcing the obligations of manufacturers or providers of ICT products, ICT services, ICT processes or managed security services pursuant to Article	(c) the procedures for monitoring and enforcing the obligations of manufacturers or providers of ICT products, ICT services, ICT processes or managed security services pursuant to Article

	Commission Proposal	EP Mandate	Council Mandate
	58(7), point (b);; ,	58(7), point (b);; ,	58(7), point (b);; ,
Article 1, first paragraph, point (16b)			
127a		***(16b) the following article is inserted:***	
Article 1, first paragraph, point (16b), amending provision, article			
127b		***Article*** ‘ ***‘Article 65a*** ***Exercise of the delegation***	
Article 1, first paragraph, point (16b), amending provision, article, first paragraph			
127c		***1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.***	
Article 1, first paragraph, point (16b), amending provision, article, second paragraph			
127d		***2. The power to adopt delegated acts referred to in Article 49(7) shall be conferred on the Commission for a period of five years from … [date of entry into force of the amended regulation]. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five year period. The delegation of power shall***	

	Commission Proposal	EP Mandate	Council Mandate
		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.	
Article 1, first paragraph, point (16b), amending provision, article, third paragraph			
127e		***3. The delegation of power referred to in Article 49(7) 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.***	
Article 1, first paragraph, point (16b), amending provision, article, fourth paragraph			
127f		***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.***	
Article 1, first paragraph, point (16b), amending provision, article, fifth paragraph			
127g		***5. As soon as it adopts a delegated act, the***	

	Commission Proposal	EP Mandate	Council Mandate
		Commission shall notify it simultaneously to the European Parliament and to the Council.	
Article 1, first paragraph, point (16b), amending provision, article, sixth paragraph			
127h		***6. A delegated act adopted pursuant to Article 49(7) 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.;'*** ,	
Article 1, first paragraph, point (17)			
128	(17) in Article 67, paragraphs 2 and 3 are replaced by the following:	(17) ~~*in*~~ Article 67~~*, paragraphs 2 and 3 are*~~ ***is*** replaced by the following:	(17) in Article 67, paragraphs 2 and 3 are replaced by the following:
Article 1, first paragraph, point (17a)			
128a		This line will be deleted by the technical service of TTE.	

	Commission Proposal	EP Mandate	Council Mandate
Article 1, first paragraph, point (18)			
128b			
Article 1, first paragraph, point (17a), amending provision, Article			
128c		***Article*** ‘ ***‘Article 67*** ***Evaluation and review***	
Article 1, first paragraph, point (17a), amending provision, Article(1)			
128d		***1. By 28 June 2024, and every three years thereafter, the Commission shall assess 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.***	
Article 1, first paragraph, point (17a), amending provision, numbered paragraph (2)			

	Commission Proposal	EP Mandate	Council Mandate
129	‘ 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.	‘ 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.
Article 1, first paragraph, point (17a), amending provision, numbered paragraph (3)			
130	3. The evaluation shall assess whether essential cybersecurity requirements for access to the internal market are necessary in order to prevent ICT products, ICT services, ICT processes and managed security services which do not meet basic cybersecurity requirements from entering the Union market.. ’	3. The evaluation shall ~~*assess whether essential cybersecurity requirements for access to the internal market are necessary in order to prevent ICT products, ICT services, ICT processes and managed security services which do not meet basic cybersecurity requirements from entering the Union market..*~~ ***also assess:***	3. The evaluation shall assess whether essential cybersecurity requirements for access to the internal market are necessary in order to prevent ICT products, ICT services, ICT processes and managed security services which do not meet basic cybersecurity requirements from entering the Union market.. ’
Article 1, first paragraph, point (17a), amending provision, Article(3), point (a)			
130a		***(a) the efficiency and effectiveness of the procedures leading to consultation, preparation and adoption of European cybersecurity certification schemes, as well as ways to improve and accelerate those procedures;***	

	Commission Proposal	EP Mandate	Council Mandate
Article 1, first paragraph, point (17a), amending provision, Article(3), point (b)			
130b		***(b) whether essential cybersecurity requirements for access to the internal market are necessary in order to prevent ICT products, ICT services, ICT processes and managed security services which do not meet basic cybersecurity requirements from entering the Union market.***	
Article 1, first paragraph, point (17a), amending provision, Article(4)			
130c		***4. By 28 June 2024, and every three 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.'*** ,	
Article 1, first paragraph, point (17b)			
130d			**(17b) the Annex shall be replaced by the text set out in the Annex to this Regulation.**
Article 2			
131	Article 2	Article 2	Article 2

	Commission Proposal	EP Mandate	Council Mandate
Article 2, first paragraph			
132	This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.	This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.	This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.
Article 2, second paragraph			
133	This Regulation shall be binding in its entirety and directly applicable in all Member States.	This Regulation shall be binding in its entirety and directly applicable in all Member States.	This Regulation shall be binding in its entirety and directly applicable in all Member States.
Formula			
134	Done at Strasbourg,	Done at Strasbourg,	Done at Strasbourg,
Formula			
135	For the European Parliament	For the European Parliament	For the European Parliament
Formula			
136	The President	The President	The President
Formula			
137	For the Council	For the Council	For the Council
Formula			

	Commission Proposal	EP Mandate	Council Mandate
138	The President	The President	The President
Annex -1			
138a			**ANNEX** **REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES**
Annex -1, first paragraph			
138b			**Conformity assessment bodies that wish to be accredited shall meet the following requirements:**
Annex -1, point 1.			
138c			**1. A conformity assessment body shall be established under national law and shall have legal personality.**
Annex -1, point 2.			
138d			**2. A conformity assessment body shall be a third-party body that is independent of the organisation or the ICT products, ICT services, ICT processes or managed security services that it assesses.**

	Commission Proposal	EP Mandate	Council Mandate
Annex -1, point 3.			
138e			**3. A body that belongs to a business association or professional federation representing undertakings involved in the design, manufacturing, provision, assembly, use or maintenance of ICT products, ICT services, ICT processes or managed security services which it assesses may be considered to be a conformity assessment body, provided that its independence and the absence of any conflict of interest are demonstrated.**
Annex -1, point 4.			
138f			**4. The conformity assessment bodies, their top-level management and the persons responsible for carrying out the conformity assessment tasks shall not be the designer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the ICT product, ICT service, ICT process or managed security service which is assessed, or the authorised representative of any of those parties. That prohibition shall not preclude the use of the ICT products assessed that are necessary for the operations of the conformity assessment body or the use of such ICT products for personal purposes.**
Annex -1, point 5.			

	Commission Proposal	EP Mandate	Council Mandate
138g			**5. The conformity assessment bodies, their top-level management and the persons responsible for carrying out the conformity assessment tasks shall not be directly involved in the design, manufacture or construction, the provision, the marketing, installation, use or maintenance of the ICT products, ICT services, ICT processes or managed security services which are assessed, or represent parties engaged in those activities. The conformity assessment bodies, their top-level management and the persons responsible for carrying out the conformity assessment tasks shall not engage in any activity that may conflict with their independence of judgement or integrity in relation to their conformity assessment activities. That prohibition shall apply, in particular, to consultancy services.**
Annex -1, point 6.			
138h			**6. If a conformity assessment body is owned or operated by a public entity or institution, the independence and absence of any conflict of interest shall be ensured between the national cybersecurity certification authority and the conformity assessment body, and shall be documented.**
Annex -1, point 7.			

	Commission Proposal	EP Mandate	Council Mandate
138i			**7. Conformity assessment bodies shall ensure that the activities of their subsidiaries and subcontractors do not affect the confidentiality, objectivity or impartiality of their conformity assessment activities.**
Annex -1, point 8.			
138j			**8. Conformity assessment bodies and their staff shall carry out conformity assessment activities with the highest degree of professional integrity and the requisite technical competence in the specific field, and shall be free from all pressures and inducements which might influence their judgement or the results of their conformity assessment activities, including pressures and inducements of a financial nature, especially as regards persons or groups of persons with an interest in the results of those activities.**
Annex -1, point 9.			
138k			**9. A conformity assessment body shall be capable of carrying out all the conformity assessment tasks assigned to it under this Regulation, regardless of whether those tasks are carried out by the conformity assessment body itself or on its behalf and under its responsibility. Any subcontracting to, or consultation of, external staff shall be**

	Commission Proposal	EP Mandate	Council Mandate
			properly documented, shall not involve any intermediaries and shall be subject to a written agreement covering, among other things, confidentiality and conflicts of interest. The conformity assessment body in question shall take full responsibility for the tasks performed.
Annex -1, point 10.			
138l			**10. At all times and for each conformity assessment procedure and each type, category or sub-category of ICT products, ICT services, ICT processes or managed security services, a conformity assessment body shall have at its disposal the necessary:**
Annex -1, point 10 (a)			
138m			**(a) staff with technical knowledge and sufficient and appropriate experience to perform the conformity assessment tasks;**
Annex -1, point 10 (b)			
138n			**(b) descriptions of procedures in accordance with which conformity assessment is to be carried out, to ensure the transparency of those procedures and the possibility of reproducing them. It shall have in place appropriate policies and procedures that**

	Commission Proposal	EP Mandate	Council Mandate
			distinguish between tasks that it carries out as a body notified pursuant to Article 61 and its other activities;
Annex -1, point 10 (c)			
138o			**(c) procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the technology of the ICT product, ICT service, ICT process or managed security service in question and the mass or serial nature of the production process.**
Annex -1, point 11.			
138p			**11. A conformity assessment body shall have the means necessary to perform the technical and administrative tasks connected with the conformity assessment activities in an appropriate manner, and shall have access to all necessary equipment and facilities.**
Annex -1, point 12.			
138q			**12. The persons responsible for carrying out conformity assessment activities shall have the following:**

	Commission Proposal	EP Mandate	Council Mandate
Annex -1, point 12 (a)			
138r			**(a) sound technical and vocational training covering all conformity assessment activities;**
Annex -1, point 12 (b)			
138s			**(b) satisfactory knowledge of the requirements of the conformity assessments they carry out and adequate authority to carry out those assessments;**
Annex -1, point 12 (c)			
138t			**(c) appropriate knowledge and understanding of the applicable requirements and testing standards;**
Annex -1, point 12 (d)			
138u			**(d) the ability to draw up certificates, records and reports demonstrating that conformity assessments have been carried out.**
Annex -1, point 13.			
138v			**13. The impartiality of the conformity assessment bodies, of their top-level management, of the persons responsible for**

	Commission Proposal	EP Mandate	Council Mandate
			carrying out conformity assessment activities, and of any subcontractors shall be guaranteed.
Annex -1, point 14.			
138w			**14. The remuneration of the top-level management and of the persons responsible for carrying out conformity assessment activities shall not depend on the number of conformity assessments carried out or on the results of those assessments.**
Annex -1, point 15.			
138x			**15. Conformity assessment bodies shall take out liability insurance unless liability is assumed by the Member State in accordance with its national law, or the Member State itself is directly responsible for the conformity assessment.**
Annex -1, point 16.			
138y			**16. The conformity assessment body and its staff, its committees, its subsidiaries, its subcontractors, and any associated body or the staff of external bodies of a conformity assessment body shall maintain confidentiality and observe professional secrecy with regard to all information**

	Commission Proposal	EP Mandate	Council Mandate
			obtained in carrying out their conformity assessment tasks under this Regulation or pursuant to any provision of national law giving effect to this Regulation, except where disclosure is required by Union or Member State law to which such persons are subject, and except in relation to the competent authorities of the Member States in which its activities are carried out. Intellectual property rights shall be protected. The conformity assessment body shall have documented procedures in place in respect of the requirements of this point.
Annex -1, point 17.			
138z			**17. With the exception of point 16, the requirements of this Annex shall not preclude exchanges of technical information and regulatory guidance between a conformity assessment body and a person who applies for certification or who is considering whether to apply for certification.**
Annex -1, point 18.			
138aa			**18. Conformity assessment bodies shall operate in accordance with a set of consistent, fair and reasonable terms and conditions, taking into account the interests of SMEs in relation to fees.**

	Commission Proposal	EP Mandate	Council Mandate
Annex -1, point 19.			
138ab			**19. Conformity assessment bodies shall meet the requirements of the relevant standard that is harmonised under Regulation (EC) No 765/2008 for the accreditation of conformity assessment bodies performing certification of ICT products, ICT services, ICT processes or managed security services.**
Annex -1, point 20.			
138ac			**20. Conformity assessment bodies shall ensure that testing laboratories used for conformity assessment purposes meet the requirements of the relevant standard that is harmonised under Regulation (EC) No 765/2008 for the accreditation of laboratories performing testing.**