Council of the European Union
General Secretariat

PUBLIC

Interinstitutional files:
2026/0011 (COD)

Brussels, 27 May 2026

WK 7571/2026 INIT

LIMITE

CYBER	**IND**
JAI	**CADREFIN**
DATAPROTECT	**FIN**
TELECOM	**BUDGET**
MI	**CSC**
	CODEC

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

WORKING DOCUMENT

From: To:	Presidency Horizontal Working Party on cyber issues (attachés)
N° Cion doc.:	ST 5611 2026 ADD 1 + ST 5611 2026 ADD 2 + ST 5611 2026 ADD 3 + ST 5611 2026 ADD 4 + ST 5611 2026 INIT
Subject:	Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2) - Presidency compromise text Titles II and III

Delegations will find in the annex a Presidency compromise text regarding Titles II (“The European Agency for Cybersecurity”, Articles 3-70) and III (“European Cybersecurity Certification Framework”, Articles 71-97). Titles IV ("Security of ICT Supply Chains") and V ("Final Provisions") as well as the annexes are not included in this compromise text.

The compromise text also includes a number of amendments to the recitals. These amendments are linked to changes in the operative part of the text, notably regarding certification. All recitals are, however, still to be revisited at a later stage of the discussions.

The changes are indicated as compared to the Commission proposals and marked in **bold** or ~~strikethrough~~.

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2) (Text with EEA relevance)

2026/0011(COD)

DRAFT [Text after drafting session 26 May]

27-05-2026 at 12h39

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Formula		
1	2026/0011 (COD)	2026/0011 (COD)
Document Stage		
2	Proposal for a	Proposal for a
Document Type		
3	REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL	REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
Document Purpose		
4	on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2)	on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2)
EEA Relevance		
5	(Text with EEA relevance)	(Text with EEA relevance)
Formula		
6	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Citation 1		

	CLEAN Commission Proposal	VS.EC Council Mandate
7	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,
Citation 2		
8	Having regard to the proposal from the European Commission,	Having regard to the proposal from the European Commission,
Citation 3		
9	After transmission of the draft legislative act to the national parliaments,	After transmission of the draft legislative act to the national parliaments,
Citation 4		
10	Having regard to the opinion of the European Economic and Social Committee[1], _____ 1. OJ C , , p. .	Having regard to the opinion of the European Economic and Social Committee[1], _____ 1. OJ C , , p. .
Citation 5		
11	Having regard to the opinion of the Committee of the Regions[1], _____ 1. OJ C , , p. .	Having regard to the opinion of the Committee of the Regions[1], _____ 1. OJ C , , p. .
Citation 6		
12	Acting in accordance with the ordinary legislative procedure,	Acting in accordance with the ordinary legislative procedure,
Formula		
13	Whereas:	Whereas:
Recital 1		
14	(1) Since the adoption of Regulation (EU) 2019/881 of the European Parliament and of the Council[1], the geopolitical, technological and policy landscapes have undergone significant transformations. Cybersecurity incidents, whether caused by system failures, human error, malicious acts or natural phenomena, have surged and cyberattacks have become more sophisticated, affecting essential entities, businesses, and the general public. The cybercrime	(1) Since the adoption of Regulation (EU) 2019/881 of the European Parliament and of the Council[1], the geopolitical, technological and policy landscapes have undergone significant transformations. Cybersecurity incidents, whether caused by system failures, human error, malicious acts or natural phenomena, have surged and cyberattacks have become more sophisticated, affecting essential entities, businesses, and the general public. The cybercrime

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	ecosystem has proliferated, with ransomware activity at its core. Supply chain incidents, whether caused by criminals for financial gain or by State actors for disruption, espionage, disinformation or warfare have intensified. As part of a wider hybrid strategy, incidents resulting from malicious cyber activities and system failures ripple outward, disrupting essential services, undermining trust in institutions, and affecting the Union's societal and defence readiness. Such incidents have proved their potential to impact economic activity, financial stability and people's lives. At the same time, vulnerability of critical civilian infrastructure and systems pose a risk to defence capabilities where they rely on them. _____ 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, ELI: http://data.europa.eu/eli/reg/2019/881/oj).	ecosystem has proliferated, with ransomware activity at its core. Supply chain incidents, whether caused by criminals for financial gain or by State actors for disruption, espionage, disinformation or warfare have intensified. As part of a wider hybrid strategy, incidents resulting from malicious cyber activities and system failures ripple outward, disrupting essential services, undermining trust in institutions, and affecting the Union's societal and defence readiness. Such incidents have proved their potential to impact economic activity, financial stability and people's lives. At the same time, vulnerability of critical civilian infrastructure and systems pose a risk to defence capabilities where they rely on them. _____ 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, ELI: http://data.europa.eu/eli/reg/2019/881/oj).
Recital 2		
15	(2) In parallel, emerging technologies such as artificial intelligence and quantum computing have a disruptive effect on cybersecurity and cyber defence. They are reshaping the tools of defence and the tactics of adversaries, posing threats to cybersecurity and cyber defence while also offering avenues for technological advancements. Although they may contribute to cybersecurity through enhanced threat detection or automated incident response, they are also increasing the overall attack surface for organisations, are potential targets for manipulation, and can undermine the long-term viability of security measures such as encryption.	(2) In parallel, emerging technologies such as artificial intelligence and quantum computing have a disruptive effect on cybersecurity and cyber defence. They are reshaping the tools of defence and the tactics of adversaries, posing threats to cybersecurity and cyber defence while also offering avenues for technological advancements. Although they may contribute to cybersecurity through enhanced threat detection or automated incident response, they are also increasing the overall attack surface for organisations, are potential targets for manipulation, and can undermine the long-term viability of security measures such as encryption.
Recital 3		
16	(3) To address those developments, the Union has enhanced its legal and policy tools. Directive (EU) 2022/2555 of the European Parliament and of the Council[1] strengthens cybersecurity for critical infrastructure, complemented by Directive (EU) 2022/2557 of the European Parliament and of the Council[2] for	(3) To address those developments, the Union has enhanced its legal and policy tools. Directive (EU) 2022/2555 of the European Parliament and of the Council[1] strengthens cybersecurity for critical infrastructure, complemented by Directive (EU) 2022/2557 of the European Parliament and of the Council[2] for

	CLEAN Commission Proposal	VS.EC Council Mandate
	physical security. Regulation (EU) 2024/2847 of the European Parliament and of the Council[3] enhances the cybersecurity of products with digital elements. Regulation (EU) 2025/38 of the European Parliament and of the Council[4] builds Union-wide response capabilities, and the Council Recommendation of 6 June 2025 on an EU blueprint for cyber crisis management[5] ('Recommendation on the Cyber Blueprint') supports Union-level crisis management cooperation. The 5G Cybersecurity Toolbox[6] constitutes a first step towards a coordinated approach at Union level to secure 5G networks. The Commission communication on the Cybersecurity Skills Academy[7] addresses the growing challenge of the cybersecurity talent gap. Additionally, the cybersecurity framework has been enhanced by sector-specific legislation, in particular Regulation (EU) 2022/2554 of the European Parliament and of the Council[8] for the financial sector, Commission Delegated Regulation (EU) 2024/1366[9] for the electricity subsector, Commission Delegated Regulation (EU) 2022/1645[10] and Commission Implementing Regulation (EU) 2023/203[11](PART-IS) as well as relevant aviation security rules set out in Commission Regulation (EU) 2019/1583[12] for the air transport sub-sector, and other policy documents such as the Commission communication on an EU action plan on the cybersecurity of hospitals and healthcare providers[13]. Union entities are also strengthened with Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council[14], which lays down measures that aim to achieve a high common level of cybersecurity within Union institutions, bodies, offices and agencies. This enhanced legal framework for cybersecurity has further specified ENISA's tasks. _____ 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, ELI: http://data.europa.eu/eli/dir/2022/2555/oj). 2. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJ L 333, 27.12.2022, p. 164, ELI: http://data.europa.eu/eli/dir/2022/2557/oj).	physical security. Regulation (EU) 2024/2847 of the European Parliament and of the Council[3] enhances the cybersecurity of products with digital elements. Regulation (EU) 2025/38 of the European Parliament and of the Council[4] builds Union-wide response capabilities, and the Council Recommendation of 6 June 2025 on an EU blueprint for cyber crisis management[5] ('Recommendation on the Cyber Blueprint') supports Union-level crisis management cooperation. The 5G Cybersecurity Toolbox[6] constitutes a first step towards a coordinated approach at Union level to secure 5G networks. The Commission communication on the Cybersecurity Skills Academy[7] addresses the growing challenge of the cybersecurity talent gap. Additionally, the cybersecurity framework has been enhanced by sector-specific legislation, in particular Regulation (EU) 2022/2554 of the European Parliament and of the Council[8] for the financial sector, Commission Delegated Regulation (EU) 2024/1366[9] for the electricity subsector, Commission Delegated Regulation (EU) 2022/1645[10] and Commission Implementing Regulation (EU) 2023/203[11](PART-IS) as well as relevant aviation security rules set out in Commission Regulation (EU) 2019/1583[12] for the air transport sub-sector, and other policy documents such as the Commission communication on an EU action plan on the cybersecurity of hospitals and healthcare providers[13]. Union entities are also strengthened with Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council[14], which lays down measures that aim to achieve a high common level of cybersecurity within Union institutions, bodies, offices and agencies. This enhanced legal framework for cybersecurity has further specified ENISA's tasks. _____ 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, ELI: http://data.europa.eu/eli/dir/2022/2555/oj). 2. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJ L 333, 27.12.2022, p. 164, ELI: http://data.europa.eu/eli/dir/2022/2557/oj).

	CLEAN Commission Proposal	VS.EC Council Mandate
	3. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj). 4. Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act) (OJ L, 2025/38, 15.01.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj). 5. OJ C, C/2025/3445, 20.6.2025, ELI: http://data.europa.eu/eli/C/2025/3445/oj. 6. Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures, NIS Cooperation Group, 1/2020, available at: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures. 7. Communication from the Commission to the European Parliament and the Council, Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience ('The Cybersecurity Skills Academy'), COM(2023)207 final, 18 April 2023. 8. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj). 9. Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows (OJ L, 2024/1366, 24.05.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj). 10. Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 748/2012 and (EU) No 139/2014 and amending Commission Regulations (EU) No 748/2012 and (EU) No 139/2014 (OJ L 248, pp. 18–31, 26.9.2022, ELI: http://data.europa.eu/eli/reg_del/2022/1645/oj). 11. Commission Implementing Regulation (EU) 2023/203 of 27 October 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664, and for competent authorities covered by Commission	3. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj). 4. Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act) (OJ L, 2025/38, 15.01.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj). 5. OJ C, C/2025/3445, 20.6.2025, ELI: http://data.europa.eu/eli/C/2025/3445/oj. 6. Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures, NIS Cooperation Group, 1/2020, available at: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures. 7. Communication from the Commission to the European Parliament and the Council, Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience ('The Cybersecurity Skills Academy'), COM(2023)207 final, 18 April 2023. 8. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj). 9. Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows (OJ L, 2024/1366, 24.05.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj). 10. Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 748/2012 and (EU) No 139/2014 and amending Commission Regulations (EU) No 748/2012 and (EU) No 139/2014 (OJ L 248, pp. 18–31, 26.9.2022, ELI: http://data.europa.eu/eli/reg_del/2022/1645/oj). 11. Commission Implementing Regulation (EU) 2023/203 of 27 October 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664, and for competent authorities covered by Commission

	CLEAN Commission Proposal	VS.EC Council Mandate
	Regulations (EU) No 748/2012, (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340 and (EU) No 139/2014, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664 and amending Commission Regulations (EU) No 1178/2011, (EU) No 748/2012, (EU) No 965/2012, (EU) No 139/2014, (EU) No 1321/2014, (EU) 2015/340, and Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664 (OJ L 31, 2.2.2023, p. 1, ELI: http://data.europa.eu/eli/reg_impl/2023/203/oj). 12. Commission Implementing Regulation (EU) 2019/1583 of 25 September 2019 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures (OJ L 246, 26.9.2019, pp. 15–18, ELI: http://data.europa.eu/eli/reg_impl/2019/1583/oj). 13. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European action plan on the cybersecurity of hospitals and healthcare providers, COM(2025) 10 final, 15 January 2025. 14. Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (OJ L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).	Regulations (EU) No 748/2012, (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340 and (EU) No 139/2014, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664 and amending Commission Regulations (EU) No 1178/2011, (EU) No 748/2012, (EU) No 965/2012, (EU) No 139/2014, (EU) No 1321/2014, (EU) 2015/340, and Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664 (OJ L 31, 2.2.2023, p. 1, ELI: http://data.europa.eu/eli/reg_impl/2023/203/oj). 12. Commission Implementing Regulation (EU) 2019/1583 of 25 September 2019 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures (OJ L 246, 26.9.2019, pp. 15–18, ELI: http://data.europa.eu/eli/reg_impl/2019/1583/oj). 13. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European action plan on the cybersecurity of hospitals and healthcare providers, COM(2025) 10 final, 15 January 2025. 14. Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (OJ L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).
Recital 4		
17	(4) In this context, and as stated in the ProtectEU: European Internal Security Strategy[1], Preparedness Union Strategy[2], ensuring the preparedness, security and resilience of the Union's society and economy requires strong European coordination, trust and information sharing between stakeholders, robust frameworks to ensure the security of ICT products, services, processes and managed security services, as well as growing and strengthening the cybersecurity workforce. It further calls for bolstering ICT supply chains by ensuring European technological sovereignty over key assets, which would increase the Union's resilience and could benefit cyber defence efforts. In addition, the Communication on Strengthening EU economic security[3] identifies as priority objectives the needs to prevent access to sensitive information and data that could undermine the EU's economic security and to prevent and mitigate disruptions to EU critical infrastructure affecting the EU economy. It acknowledges the essential role effective cybersecurity measures play in this regard.	(4) In this context, and as stated in the ProtectEU: European Internal Security Strategy[1], Preparedness Union Strategy[2], ensuring the preparedness, security and resilience of the Union's society and economy requires strong European coordination, trust and information sharing between stakeholders, robust frameworks to ensure the security of ICT products, services, processes and managed security services, as well as growing and strengthening the cybersecurity workforce. It further calls for bolstering ICT supply chains by ensuring European technological sovereignty over key assets, which would increase the Union's resilience and could benefit cyber defence efforts. In addition, the Communication on Strengthening EU economic security[3] identifies as priority objectives the needs to prevent access to sensitive information and data that could undermine the EU's economic security and to prevent and mitigate disruptions to EU critical infrastructure affecting the EU economy. It acknowledges the essential role effective cybersecurity measures play in this regard.

	CLEAN Commission Proposal	VS.EC Council Mandate
	_____ 1. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Protect EU: a European Internal Security Strategy, COM(2025)148 final, 1 April 2025. 2. Joint Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Preparedness Union Strategy, JOIN(2025) 130 final. 3. Joint Communication from the Commission to the European Parliament and the Council, Strengthening EU economic security, JOIN(2025) 977 final.	_____ 1. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Protect EU: a European Internal Security Strategy, COM(2025)148 final, 1 April 2025. 2. Joint Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Preparedness Union Strategy, JOIN(2025) 130 final. 3. Joint Communication from the Commission to the European Parliament and the Council, Strengthening EU economic security, JOIN(2025) 977 final.
Recital 5		
18	(5) Large-scale cybersecurity incidents affecting critical infrastructure, digital services or essential societal functions may have impacts on the population requiring coordinated civil protection and crisis management action at Union level. In line with the all-hazards approach of the European Preparedness Union Strategy and Decision No 1313/2013/EU on the Union Civil Protection Mechanism, arrangements for situational awareness, incident response and exercises under this Regulation should feed in Union crisis management, notably though the Emergency Response Coordination Centre (ERCC).	(5) Large-scale cybersecurity incidents affecting critical infrastructure, digital services or essential societal functions may have impacts on the population requiring coordinated civil protection and crisis management action at Union level. In line with the all-hazards approach of the European Preparedness Union Strategy and Decision No 1313/2013/EU on the Union Civil Protection Mechanism, arrangements for situational awareness, incident response and exercises under this Regulation should feed in Union crisis management, notably though the Emergency Response Coordination Centre (ERCC).
Recital 6		
19	(6) This proposal is consistent with and complemented by the [Proposal for a Directive complementing [the revision of Regulation (EU) 2019/881] and amending Directive (EU) 2022/2555 as regards the simplification of the implementation of measures for a high common level of cybersecurity across the Union], as well as with the [Proposal for Regulation on simplification of the digital legislation (Digital Omnibus)[1] which provides the obligation on ENISA to develop a single entry-point for incident reporting through which entities can simultaneously fulfil their incident reporting obligations under multiple legal acts. _____ 1. COM/2025/837 final	(6) This proposal is consistent with and complemented by the [Proposal for a Directive complementing [the revision of Regulation (EU) 2019/881] and amending Directive (EU) 2022/2555 as regards the simplification of the implementation of measures for a high common level of cybersecurity across the Union], as well as with the [Proposal for Regulation on simplification of the digital legislation (Digital Omnibus)[1] which provides the obligation on ENISA to develop a single entry-point for incident reporting through which entities can simultaneously fulfil their incident reporting obligations under multiple legal acts. _____ 1. COM/2025/837 final

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Recital 6a		
19a		*(6a)Undertakings, organisations, manufacturers or providers involved in the design and development of ICT products, ICT services, ICT processes or managed security services should implement measures at the earliest stages of design and development to protect the security of those products, services and processes to the highest possible degree, in such a way that the occurrence of cyberattacks is presumed and their impact is anticipated and minimised ('security-by-design'). Security should be ensured throughout the lifetime of the ICT product, ICT service or ICT process as well as continuously for managed security services by design and development processes that constantly evolve to reduce the risk of harm from malicious exploitation and ensure that services are inherently secure.*
Recital 6b		
19b		*(6b)Undertakings, organisations and the public sector should configure the ICT products, ICT services, ICT processes and managed security services designed by them in a way that ensures a higher level of security which should enable the first user to receive a default configuration with the most secure settings possible ('security by default'), thereby reducing the burden on users of having to configure them appropriately. Security by default should not require extensive configuration or specific technical understanding or non-intuitive behaviour on the part of the user, and should work easily and reliably when implemented. If, on a case-by-case basis, a risk and usability analysis leads to the conclusion that such a setting by default is not feasible, users should be prompted to opt for the most secure setting.*
Recital 7		
20	(7) Regulation (EC) No 460/2004 of the European Parliament and of the Council[1] established ENISA with the aim of contributing to ensuring a high and effective level of network and information security within the Union, and developing a culture of network and information security for the benefit of	(7) Regulation (EC) No 460/2004 of the European Parliament and of the Council[1] established ENISA with the aim of contributing to ensuring a high and effective level of network and information security within the Union, and developing a culture of network and information security for the benefit of

	CLEAN Commission Proposal	VS.EC Council Mandate
	citizens, consumers, enterprises and public administrations. ENISA's mandate was extended three times before Regulation (EU) 2019/881 granted it a permanent mandate. In order to better address the needs created by the evolving threat and technological landscapes, in particular with regards to operational cooperation and the increased need for cybersecurity professionals, ENISA's mandate should be further reinforced. In the interest of legal certainty, Regulation (EU) 2019/881 should be replaced. _____ 1. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (OJ L 77, 13.3.2004, p. 1, ELI: http://data.europa.eu/eli/reg/2004/460/oj).	citizens, consumers, enterprises and public administrations. ENISA's mandate was extended three times before Regulation (EU) 2019/881 granted it a permanent mandate. In order to better address the needs created by the evolving threat and technological landscapes, in particular with regards to operational cooperation and the increased need for cybersecurity professionals, ENISA's mandate should be further reinforced. In the interest of legal certainty, Regulation (EU) 2019/881 should be replaced. _____ 1. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (OJ L 77, 13.3.2004, p. 1, ELI: http://data.europa.eu/eli/reg/2004/460/oj).
Recital 8		
21	(8) In an evolving threat landscape where cybersecurity incidents become increasingly more significant, delivering trust for individuals, public authorities and businesses in their daily use of technologies is even more important than ever. An increase in trust can be facilitated by a reinforced Union-wide certification of the ECCF providing for common cybersecurity requirements and evaluation criteria across national markets and sectors. The new framework should lay down the main horizontal requirements for European cybersecurity certification schemes and allow for European cybersecurity certificates and EU statements of conformity to be recognised and used in all Member States. In doing so, it should establish a procedure and governance framework that allows for the timely and predictable development and maintenance of European cybersecurity certification schemes. The European cybersecurity certification schemes should be applied uniformly in all Member States to ensure a harmonised implementation of cybersecurity requirements, level the playing field and prevent 'certification shopping' based on different levels of stringency in different Member States. ENISA should have a key role in providing for the development of the schemes through technical specifications and ensuring that such schemes remain technically up to date. Furthermore, to meet the market	(8) In an evolving threat landscape where cybersecurity incidents become increasingly more significant, delivering trust for individuals, public authorities and businesses in their daily use of technologies is even more important than ever. An increase in trust can be facilitated by a reinforced Union-wide certification of the ECCF providing for common cybersecurity requirements and evaluation criteria across national markets and sectors. The new framework should lay down the main horizontal requirements for European cybersecurity certification schemes and allow for European cybersecurity certificates and EU statements of conformity to be recognised and used in all Member States. In doing so, it should establish a procedure and governance framework that allows for the timely and predictable development ***in fast innovation cycles, particularly in software and AI-driven environments,*** and maintenance of European cybersecurity certification schemes. The European cybersecurity certification schemes should be applied uniformly in all Member States to ensure a harmonised implementation of cybersecurity requirements, level the playing field and prevent 'certification shopping' based on different levels of stringency in different Member States. ENISA should have a key role in providing for the development of the schemes through technical specifications and ensuring that

	CLEAN Commission Proposal	VS.EC Council Mandate
	needs effectively, the framework should provide for the possibility for certification of cybersecurity risk management measures addressed to entities and facilitate compliance with other applicable Union legislation in the field of cybersecurity. Alignment with existing Union law, such as Regulation (EU) 2024/2847 and Directive (EU) 2022/2555, is essential for European cybersecurity certification schemes to contribute to reducing compliance burden on businesses, increase their attractiveness and strengthen the cyber resilience of the Union.	such schemes remain technically up to date. Furthermore, to meet the market needs effectively, the framework should provide for the possibility for certification of cybersecurity risk management measures addressed to entities and facilitate compliance with other applicable Union legislation in the field of cybersecurity. Alignment with existing Union law, such as Regulation (EU) 2024/2847 and Directive (EU) 2022/2555, is essential for European cybersecurity certification schemes to contribute to reducing compliance burden on businesses, increase their attractiveness and strengthen the cyber resilience of the Union.
Recital 9		
22	(9) The mission of ENISA should be to support Member States and Union entities to achieve a high level of cybersecurity, resilience and trust in the Union. To that end, ENISA should act as a reference point for advice and expertise on cybersecurity, and its work should primarily revolve around four key areas of cybersecurity at Union level. First, ENISA should support Member States in the consistent implementation of Union policy and legislation regarding cybersecurity and assist Member States through capacity-building activities to continuously improve their capacities in terms of preparedness, resilience and response. Second, ENISA should contribute to operational cooperation at Union level, amongst Member States, and to enhanced shared situational awareness of cyber threats and incidents among Member States and Union entities. The third key area should be cybersecurity certification and standardisation, while the fourth should be the implementation of the Cybersecurity Skills Academy, which should contribute to the development of a thriving European cybersecurity workforce with skills that should be portable across Member States.	(9) The mission of ENISA should be to support Member States and Union entities to achieve a high level of cybersecurity, resilience and trust in the Union. To that end, ENISA should act as a reference point for advice and expertise on cybersecurity, and its work should primarily revolve around four key areas of cybersecurity at Union level. First, ENISA should support Member States in the consistent implementation of Union policy and legislation regarding cybersecurity and assist Member States through capacity-building activities to continuously improve their capacities in terms of preparedness, resilience and response. Second, ENISA should contribute to operational cooperation at Union level, amongst Member States, and to enhanced shared situational awareness of cyber threats and incidents among Member States and Union entities. The third key area should be cybersecurity certification and standardisation, while the fourth should be the implementation of the Cybersecurity Skills Academy, which should contribute to the development of a thriving European cybersecurity workforce with skills that should be portable across Member States.
Recital 10		
23	(10) Regulation (EU, Euratom) 2023/2841 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union and provides for the mandate of CERT-EU, establishing it as the	(10) Regulation (EU, Euratom) 2023/2841 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union and provides for the mandate of CERT-EU, establishing it as the

	CLEAN Commission Proposal	VS.EC Council Mandate
	Cybersecurity Service for Union institutions, bodies, offices and agencies to contribute to the security of the unclassified ICT environment of Union entities by advising them on cybersecurity, supporting them to prevent, detect, handle, mitigate, respond to and recover from incidents and acting as their cybersecurity information exchange and incident response coordination hub. Furthermore, CERT-EU is tasked with offering relevant cybersecurity services to Union entities. As part of its mission, ENISA should support also Union entities. In particular, it should do so by engaging through structured cooperation with CERT-EU on capacity building, operational cooperation and long-term strategic analyses of cyber threats. When relevant, ENISA may leverage the structured cooperation with CERT-EU for ENISA cybersecurity services or support that can be of added value to Union entities, in a coordinated manner to ensure synergies of efforts of CERT-EU.	Cybersecurity Service for Union institutions, bodies, offices and agencies to contribute to the security of the unclassified ICT environment of Union entities by advising them on cybersecurity, supporting them to prevent, detect, handle, mitigate, respond to and recover from incidents and acting as their cybersecurity information exchange and incident response coordination hub. Furthermore, CERT-EU is tasked with offering relevant cybersecurity services to Union entities. As part of its mission, ENISA should support also Union entities. In particular, it should do so by engaging through structured cooperation with CERT-EU on capacity building, operational cooperation and long-term strategic analyses of cyber threats. When relevant, ENISA may leverage the structured cooperation with CERT-EU for ENISA cybersecurity services or support that can be of added value to Union entities, in a coordinated manner to ensure synergies of efforts of CERT-EU.
Recital 11		
24	(11) One of the core tasks of ENISA should be to support Member States in implementing Union policy and law regarding cybersecurity consistently, in particular as regards Directive (EU) 2022/2555, Regulation (EU) 2024/2847, and Regulation (EU) 2025/38. To help achieve consistent and effective implementation of the Union cybersecurity acquis, ENISA should issue technical guidance and reports, provide advice and best practices, and facilitate the exchange of best practices between competent authorities to this end. Furthermore, ENISA is assessing the state of cybersecurity in the Union and adopts a report to that end in accordance with Article 18 of Directive (EU) 2022/2555. ENISA should also be able to respond to requests for advice and assistance by Member States and, where applicable, Union entities, on matters falling within ENISA's mandate.	(11) One of the core tasks of ENISA should be to support Member States in implementing Union policy and law regarding cybersecurity consistently, in particular as regards Directive (EU) 2022/2555, Regulation (EU) 2024/2847, and Regulation (EU) 2025/38. To help achieve consistent and effective implementation of the Union cybersecurity acquis, ENISA should issue technical guidance and reports, provide advice and best practices, and facilitate the exchange of best practices between competent authorities to this end. Furthermore, ENISA is assessing the state of cybersecurity in the Union and adopts a report to that end in accordance with Article 18 of Directive (EU) 2022/2555. ENISA should also be able to respond to requests for advice and assistance by Member States and, where applicable, Union entities, on matters falling within ENISA's mandate.
Recital 12		
25	(12) With a view to stimulating cooperation between the public and private sectors and within the private sector, in particular to support the protection of	(12) With a view to stimulating cooperation between the public and private sectors and within the private sector, in particular to support the protection of

	CLEAN Commission Proposal	VS.EC Council Mandate
	critical infrastructure, ENISA should support information sharing within and among sectors, in particular the sectors listed in Annexes I and II to Directive (EU) 2022/2555, and information regarding products with digital elements falling within the scope of Regulation (EU) 2024/2847. Such support may take the form of providing best practices and guidance on available tools and procedures, as well as providing guidance on how to address regulatory issues related to information sharing, for example through facilitating the establishment of sectoral Information Sharing and Analysis Centres (ISACs).	critical infrastructure, ENISA should support information sharing within and among sectors, in particular the sectors listed in Annexes I and II to Directive (EU) 2022/2555, and information regarding products with digital elements falling within the scope of Regulation (EU) 2024/2847. Such support may take the form of providing best practices and guidance on available tools and procedures, as well as providing guidance on how to address regulatory issues related to information sharing, for example through facilitating the establishment of sectoral Information Sharing and Analysis Centres (ISACs).
Recital 13		
26	(13) In view of supporting and facilitating the strategic cooperation and the exchange of information, ENISA should contribute to the work of the Cooperation Group established by Directive (EU) 2022/2555 ('NIS Cooperation Group'), in particular by providing expertise, advice and by facilitating the exchange of best practices, among others, in relation to cross-border dependencies, regarding risks and incidents. ENISA should also contribute to the work of the European Digital Identity Cooperation Group established by Regulation (EU) No 910/2014 of the European Parliament and of the Council[1], the European Cybersecurity Certification Group, and the administrative cooperation group (ADCO) established by Regulation (EU) 2024/2847. _____ 1. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).	(13) In view of supporting and facilitating the strategic cooperation and the exchange of information, ENISA should contribute to the work of the Cooperation Group established by Directive (EU) 2022/2555 ('NIS Cooperation Group'), in particular by providing expertise, advice and by facilitating the exchange of best practices, among others, in relation to cross-border dependencies, regarding risks and incidents. ENISA should also contribute to the work of the European Digital Identity Cooperation Group established by Regulation (EU) No 910/2014 of the European Parliament and of the Council[1], the European Cybersecurity Certification Group, and the administrative cooperation group (ADCO) established by Regulation (EU) 2024/2847. _____ 1. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).
Recital 14		
27	(14) The public core of the open internet, namely its main protocols and infrastructure, which are a global public good, provides the essential functionality of the internet as a whole and underpins its normal operation. Within its	(14) The public core of the open internet, namely its main protocols and infrastructure, which are a global public good, provides the essential functionality of the internet as a whole and underpins its normal operation. Within its

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	mandate, ENISA should support the security and resilience of the public core of the open internet and the stability of its functioning, including, but not limited to, the secure deployment and operation of key protocols (in particular Domain Name System, Border Gateway Protocol, and Internet Protocol version 6) and the operation of the domain name system (such as the operation of all top-level domains), by promoting best practices, guidance, and cooperation, in accordance with established global, multistakeholder Internet governance arrangements and the respective roles and responsibilities of relevant international technical and operational bodies.	mandate, ENISA should support the security and resilience of the public core of the open internet and the stability of its functioning, including, but not limited to, the secure deployment and operation of key protocols (in particular Domain Name System, Border Gateway Protocol, and Internet Protocol version 6) and the operation of the domain name system (such as the operation of all top-level domains), by promoting best practices, guidance, and cooperation, in accordance with established global, multistakeholder Internet governance arrangements and the respective roles and responsibilities of relevant international technical and operational bodies.
Recital 15		
28	(15) ENISA acts as a reference point for advice and expertise on cybersecurity. Therefore, at the Commission's request, ENISA should assist it by means of expertise, technical advice, information, analyses, including feasibility studies, opinions and preparatory work regarding any specific matter in the field of cybersecurity with a view to informing the Commission's policymaking and facilitating the Commission's monitoring of the implementation of Union legislation regarding cybersecurity.	(15) ENISA acts as a reference point for advice and expertise on cybersecurity. Therefore, at the Commission's request, ENISA should assist it by means of expertise, technical advice, information, analyses, including feasibility studies, opinions and preparatory work regarding any specific matter in the field of cybersecurity with a view to informing the Commission's policymaking and facilitating the Commission's monitoring of the implementation of Union legislation regarding cybersecurity.
Recital 16		
29	(16) Similarly, taking into account its expertise, ENISA should assist Member States in their efforts to build and enhance capabilities and preparedness to prevent, detect and respond to cyber threats and incidents and in relation to the security of network and information systems. In particular, ENISA should support the development and enhancement of computer security incident response teams ('CSIRTs') provided for in Directive (EU) 2022/2555, with a view to achieving a high common level of maturity of CSIRTs in the Union.	(16) Similarly, taking into account its expertise, ENISA should assist Member States in their efforts to build and enhance capabilities and preparedness to prevent, detect and respond to cyber threats and incidents and in relation to the security of network and information systems. In particular, ENISA should support the development and enhancement of computer security incident response teams ('CSIRTs') provided for in Directive (EU) 2022/2555, with a view to achieving a high common level of maturity of CSIRTs in the Union.
Recital 17		
30	(17) ENISA has supported and should continue supporting Member States in developing and implementing guidelines for their national cybersecurity	(17) ENISA has supported and should continue supporting Member States in developing and implementing guidelines for their national cybersecurity

	CLEAN Commission Proposal	VS.EC Council Mandate
	strategies contributing to the adoption and implementation of cybersecurity strategies by all Member States ENISA should promote the dissemination of such strategies through the National Cybersecurity Strategies (NCSS) Interactive Map and should further follow the progress of their implementation, including by providing support in the development of key performance indicators in this context.	strategies contributing to the adoption and implementation of cybersecurity strategies by all Member States ENISA should promote the dissemination of such strategies through the National Cybersecurity Strategies (NCSS) Interactive Map and should further follow the progress of their implementation, including by providing support in the development of key performance indicators in this context.
Recital 18		
31	(18) Regulation (EU, Euratom) 2023/2841 has tasked the Interinstitutional Cybersecurity Board with supporting Union entities in elevating their respective cybersecurity postures, and CERT-EU with contributing to the security of the unclassified ICT environment of all Union entities. ENISA, based on its experience in cybersecurity, should support the Interinstitutional Cybersecurity Board and CERT-EU in their tasks in accordance with Regulation (EU, Euratom) 2023/2841, including by contributing to cyber threat analysis, situational awareness, cybersecurity exercises, coordination on incident response and the exchange of know-how and best practices.	(18) Regulation (EU, Euratom) 2023/2841 has tasked the Interinstitutional Cybersecurity Board with supporting Union entities in elevating their respective cybersecurity postures, and CERT-EU with contributing to the security of the unclassified ICT environment of all Union entities. ENISA, based on its experience in cybersecurity, should support the Interinstitutional Cybersecurity Board and CERT-EU in their tasks in accordance with Regulation (EU, Euratom) 2023/2841, including by contributing to cyber threat analysis, situational awareness, cybersecurity exercises, coordination on incident response and the exchange of know-how and best practices.
Recital 19		
32	(19) Based on ENISA's expertise and to complement the capabilities of national and Union public authorities, ENISA should deliver training using the European Cybersecurity Skills Framework (ECSF) as a basis, in particular to support effective policy implementation, operational cooperation, and awareness-raising.	(19) Based on ENISA's expertise and to complement the capabilities of national and Union public authorities, ENISA should deliver training using the European Cybersecurity Skills Framework (ECSF) as a basis, in particular to support effective policy implementation, operational cooperation, and awareness-raising.
Recital 20		
33	(20) To ensure synergies with the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) and the Network of National Coordination Centres established pursuant to Regulation (EU) 2021/887 of the European Parliament and of the Council[1], ENISA should support them by sharing information about current and emerging risks and cyber	(20) To ensure synergies with the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) and the Network of National Coordination Centres established pursuant to Regulation (EU) 2021/887 of the European Parliament and of the Council[1], ENISA should support them by sharing information about current and emerging risks and cyber

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	threats, including risks and threats regarding information and communications technologies. _____ 1. Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (OJ L 202, 8.6.2021, p. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).	threats, including risks and threats regarding information and communications technologies. _____ 1. Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (OJ L 202, 8.6.2021, p. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).
Recital 21		
34	(21) The Preparedness Strategy highlights that digital literacy, which relies on acquiring basic digital skills, is essential to empower more resilient citizens in the face of potential crises. However, as highlighted in the Commission Communication on the Union of Skills[1], almost half the adult population does not have basic digital skills despite more than 90% of jobs requiring them. In order to ensure that the current and potential future workforce have the required skills in a rapidly evolving digital environment, and to contribute to the development of the European cybersecurity talent pipeline, ENISA should support cybersecurity awareness-raising activities that aim to attract talent and help informing about the education and skills needed in the area of cybersecurity, such as the European Cybersecurity Challenge. In this regard, ENISA should coordinate cybersecurity competitions, capture-the-flag events and similar practical exercises, as a means of developing cybersecurity skills and fostering capacity building across the Union. When carrying out awareness-raising activities, ENISA should ensure that these address the needs of national public authorities and Union entities, as well as the needs of businesses, in particular SMEs, and education and training institutions, by maintaining practical frameworks and trainings such as awareness-raising-in-a-box. ENISA should further develop practical and actionable guidance to support the implementation of Union cybersecurity policy and legislation. ENISA should also strive to provide relevant information on applicable certification schemes, for example by providing guidelines and recommendations.	(21) The Preparedness Strategy highlights that digital literacy, which relies on acquiring basic digital skills, is essential to empower more resilient citizens in the face of potential crises. However, as highlighted in the Commission Communication on the Union of Skills[1], almost half the adult population does not have basic digital skills despite more than 90% of jobs requiring them. In order to ensure that the current and potential future workforce have the required skills in a rapidly evolving digital environment, and to contribute to the development of the European cybersecurity talent pipeline, ENISA should support cybersecurity awareness-raising activities that aim to attract talent and help informing about the education and skills needed in the area of cybersecurity, such as the European Cybersecurity Challenge. In this regard, ENISA should coordinate cybersecurity competitions, capture-the-flag events and similar practical exercises, as a means of developing cybersecurity skills and fostering capacity building across the Union. When carrying out awareness-raising activities, ENISA should ensure that these address the needs of national public authorities and Union entities, as well as the needs of businesses, in particular SMEs, and education and training institutions, by maintaining practical frameworks and trainings such as awareness-raising-in-a-box. ENISA should further develop practical and actionable guidance to support the implementation of Union cybersecurity policy and legislation. ENISA should also strive to provide relevant information on applicable certification schemes, for example by providing guidelines and recommendations.

	CLEAN Commission Proposal	VS.EC Council Mandate
	_____ 1. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, The Union of Skills, COM(2025) 90 final, 5 March 2025.	_____ 1. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, The Union of Skills, COM(2025) 90 final, 5 March 2025.
Recital 22		
35	(22) To support businesses operating in the cybersecurity sector, users of cybersecurity solutions, and to ensure effective the implementation of Title III of this Regulation, ENISA should develop and maintain a 'market observatory' by performing regular analyses and disseminating information on the main trends in the cybersecurity market, on both the demand and supply sides. Furthermore, to support the users of the EU Cybersecurity Reserve established pursuant to Regulation (EU) 2025/38, ENISA should prepare the mapping of the services needed by such users, and of availability of such services, pursuant to that Regulation.	(22) To support businesses operating in the cybersecurity sector, users of cybersecurity solutions, and to ensure effective the implementation of Title III of this Regulation, ENISA should develop and maintain a 'market observatory' by performing regular analyses and disseminating information on the main trends in the cybersecurity market, on both the demand and supply sides. Furthermore, to support the users of the EU Cybersecurity Reserve established pursuant to Regulation (EU) 2025/38, ENISA should prepare the mapping of the services needed by such users, and of availability of such services, pursuant to that Regulation.
Recital 23		
36	(23) Cyber threats are a global issue. Closer international cooperation is necessary to improve cybersecurity, including to define common norms of behaviour and common approaches. To that end, ENISA should support Union's cooperation with third countries, with a focus on countries that are candidates for accession to the Union, and international organisations, such as NATO, by providing the necessary expertise and analysis to the Commission and relevant Union entities, where appropriate. ENISA's activities in the international area should always be in line with the priorities of the Union.	(23) Cyber threats are a global issue. Closer international cooperation is necessary to improve cybersecurity, including to define common norms of behaviour and common approaches. To that end, ENISA should support Union's cooperation with third countries, with a focus on countries that are candidates for accession to the Union, and international organisations, such as NATO, by providing the necessary expertise and analysis to the Commission and relevant Union entities, where appropriate. ENISA's activities in the international area should always be in line with the priorities of the Union.
Recital 24		
37	(24) To help achieve a high level of cybersecurity in the Union, ENISA should support operational cooperation among Member States, in cooperation with CERT-EU, among Union entities, and between stakeholders. To that end, ENISA's role should be strengthened. ENISA should become a member of the CSIRTs network, contributing to the network information exchange and	(24) To help achieve a high level of cybersecurity in the Union, ENISA should support operational cooperation among Member States, in cooperation with CERT-EU, among Union entities, and between stakeholders. To that end, ENISA's role should be strengthened. ENISA should become a member of the CSIRTs network, contributing to the network information exchange and

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	analysis. ENISA should further promote and support cooperation between the relevant CSIRTs in the event of incidents, attacks or disruptions of networks or infrastructure managed or protected by the CSIRTs. ENISA's active support for the work of the CSIRTs network and the European cyber crisis liaison organisation network (EU-CyCLONe) should enable those networks to continue strengthening their maturity level. ENISA's role in supporting such cooperation includes combating threats to the security and integrity of democratic institutions, elections and other processes, and the critical infrastructure on which they depend, in line with the European Democracy Shield: Empowering Strong and Resilient Democracies[1]. _____ 1. JOIN(2025) 791 final.	analysis. ENISA should further promote and support cooperation between the relevant CSIRTs in the event of incidents, attacks or disruptions of networks or infrastructure managed or protected by the CSIRTs. ENISA's active support for the work of the CSIRTs network and the European cyber crisis liaison organisation network (EU-CyCLONe) should enable those networks to continue strengthening their maturity level. ENISA's role in supporting such cooperation includes combating threats to the security and integrity of democratic institutions, elections and other processes, and the critical infrastructure on which they depend, in line with the European Democracy Shield: Empowering Strong and Resilient Democracies[1]. _____ 1. JOIN(2025) 791 final.
Recital 25		
38	(25) To support capacity-building, operational cooperation, and long-term strategic analyses of cyber threats, ENISA should make use of the available technical and operational expertise of CERT-EU through structured cooperation, for example through dedicated arrangements.	(25) To support capacity-building, operational cooperation, and long-term strategic analyses of cyber threats, ENISA should make use of the available technical and operational expertise of CERT-EU through structured cooperation, for example through dedicated arrangements.
Recital 26		
39	(26) In order to strengthen cybersecurity across the Union and ensure a rapid and effective response to cyber threats, ENISA should support Member States at their request, including by providing advice on the improvement of their capabilities to prevent, detect, respond to and recover from incidents, by facilitating the technical handling of significant incidents within the meaning of Directive (EU) 2022/2555, in particular through supporting the voluntary sharing of technical solutions between Member States, or by ensuring that cyber threats and incidents are analysed. ENISA should also assist EU-CyCLONe in preparing reports to the Union's and Member States' political level.	(26) In order to strengthen cybersecurity across the Union and ensure a rapid and effective response to cyber threats, ENISA should support Member States at their request, including by providing advice on the improvement of their capabilities to prevent, detect, respond to and recover from incidents, by facilitating the technical handling of significant incidents within the meaning of Directive (EU) 2022/2555, in particular through supporting the voluntary sharing of technical solutions between Member States, or by ensuring that cyber threats and incidents are analysed. ENISA should also assist EU-CyCLONe in preparing reports to the Union's and Member States' political level.
Recital 27		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
40	(27) To reduce exposure to foreign interference, supply-chain manipulation, and strategic data exfiltration, ENISA should use within the CSIRTs network and EU-CyCLONe secure communications tools. Building on the Recommendation on the Cyber Blueprint, such tools should be provided by legal entities established or deemed to be established in the Union and controlled by Member States or by nationals of Member States.	(27) To reduce exposure to foreign interference, supply-chain manipulation, and strategic data exfiltration, ENISA should use within the CSIRTs network and EU-CyCLONe secure communications tools. Building on the Recommendation on the Cyber Blueprint, such tools should be provided by legal entities established or deemed to be established in the Union and controlled by Member States or by nationals of Member States.
Recital 28		
41	(28) To contribute to Union-level preparedness and response in the case of large-scale cybersecurity incidents and crises, ENISA should carry out cybersecurity situational awareness activities.	(28) To contribute to Union-level preparedness and response in the case of large-scale cybersecurity incidents and crises, ENISA should carry out cybersecurity situational awareness activities.
Recital 29		
42	(29) Access to real-time, verified, reliable cyber threat intelligence (CTI) is crucial for building shared situational awareness in the Union. ENISA, the Commission, CERT-EU and the European Cybercrime Centre (EC3) at Europol have already developed repositories of cyber threat intelligence that are tailored to their specific needs. ENISA and other relevant Union entities should cooperate, voluntarily, to develop repositories of real-time, verified, reliable CTI, and seek synergies to ensure economies of scale and reinforce sound financial management. This work should also include sectoral Union entities such as the EU agency for the Space Programme. They should share only derived analysis, trends, and tactics, techniques and procedures (TTPs), not raw sources, and should respect the independence of entities to manage their own CTI lifecycle in line with their mandates and need-to-know rules.	(29) Access to real-time, verified, reliable cyber threat intelligence (CTI) is crucial for building shared situational awareness in the Union. ENISA, the Commission, CERT-EU and the European Cybercrime Centre (EC3) at Europol have already developed repositories of cyber threat intelligence that are tailored to their specific needs. ENISA and other relevant Union entities should cooperate, voluntarily, to develop repositories of real-time, verified, reliable CTI, and seek synergies to ensure economies of scale and reinforce sound financial management. This work should also include sectoral Union entities such as the EU agency for the Space Programme. They should share only derived analysis, trends, and tactics, techniques and procedures (TTPs), not raw sources, and should respect the independence of entities to manage their own CTI lifecycle in line with their mandates and need-to-know rules.
Recital 30		
43	(30) In order to contribute to a timely and coordinated response, ENISA should be able to issue early alerts of a potential or ongoing significant or large-scale incident, or a cyber threat of a potential cross-border nature to the CSIRT or CSIRTs concerned, and, where appropriate, to the CSIRTs network and EU-	(30) In order to contribute to a timely and coordinated response, ENISA should be able to issue early alerts of a potential or ongoing significant or large-scale incident, or a cyber threat of a potential cross-border nature to the CSIRT or CSIRTs concerned, and, where appropriate, to the CSIRTs network and EU-

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	CyCLONe, in particular in relation to entities listed in Annexes I and II to Directive (EU) 2022/2555. Information in such early alerts may include publicly known vulnerabilities and whether they affect products with digital elements covered by Regulation (EU) 2024/2847, as well as techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information and recommendations on mitigation measures.	CyCLONe, in particular in relation to entities listed in Annexes I and II to Directive (EU) 2022/2555. Information in such early alerts may include publicly known vulnerabilities and whether they affect products with digital elements covered by Regulation (EU) 2024/2847, as well as techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information and recommendations on mitigation measures.
Recital 31		
44	(31) In order to maintain trust and not jeopardise information-sharing, it is important for ENISA to apply visible markings indicating the extent to which a document or information it has produced or received may be shared further. Similarly, ENISA should use documents or information it receives for the purposes of carrying out its activities, subject to any limitations by means of a visible marking on further distribution of that information.	(31) In order to maintain trust and not jeopardise information-sharing, it is important for ENISA to apply visible markings indicating the extent to which a document or information it has produced or received may be shared further. Similarly, ENISA should use documents or information it receives for the purposes of carrying out its activities, subject to any limitations by means of a visible marking on further distribution of that information.
Recital 32		
45	(32) To help increase awareness of cyber threat indicators and recommendations on mitigation measures, ENISA should make an early alert service available to entities operating in sectors listed in Annexes I and II to Directive (EU) 2022/2555. Such generic, voluntary early alerts should benefit in particular SMEs, and should be provided in a machine-readable format made publicly available. In any case, such voluntary service is separate from and not related to any public-private partnerships that ENISA may establish or has already established.	(32) To help increase awareness of cyber threat indicators and recommendations on mitigation measures, ENISA should make an early alert service available to entities operating in sectors listed in Annexes I and II to Directive (EU) 2022/2555. Such generic, voluntary early alerts should benefit in particular SMEs, and should be provided in a machine-readable format made publicly available. In any case, such voluntary service is separate from and not related to any public-private partnerships that ENISA may establish or has already established.
Recital 33		
46	(33) To support Union shared cybersecurity situational awareness, ENISA, in close cooperation with the Member States, should prepare a regular in-depth EU Cybersecurity Technical Situation Report on incidents and cyber threats, based on publicly available information, its own analysis and reports shared with it by Member States' CSIRTs or the national single points of contact on the security of	(33) To support Union shared cybersecurity situational awareness, ENISA, in close cooperation with the Member States, should prepare a regular in-depth EU Cybersecurity Technical Situation Report on incidents and cyber threats, based on publicly available information, its own analysis and reports shared with it by Member States' CSIRTs or the national single points of contact on the security of

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	network and information systems ('single points of contact') provided for in Directive (EU) 2022/2555, both on a voluntary basis, Europol and CERT-EU. That report should be made available to the Council, the European External Action Service, EU-CyCLONe, the CSIRTs network, the Commission and Europol.	network and information systems ('single points of contact') provided for in Directive (EU) 2022/2555, both on a voluntary basis, Europol and CERT-EU. That report should be made available to the Council, the European External Action Service, EU-CyCLONe, the CSIRTs network, the Commission and Europol.
Recital 34		
47	(34) In order to enhance the shared situational awareness of the cyber threat and incident landscape among stakeholders, ENISA should analyse trends in cyber threats and incidents. This should include a regular analysis addressing the sectors of high criticality and other critical sectors listed in Annexes I and II to Directive (EU) 2022/2555, including the healthcare, energy and transport sectors. Such analysis should include maturity levels of sectors and identify, among others, possible challenges specific to a given sector. Where relevant, and in order to identify supply chain effects, the analysis should evidence cyber threats and trends related to product categories covered by Regulation (EU) 2024/2847. ENISA should develop expertise in the field of cybersecurity of infrastructures and their critical supply chain dependencies, in particular to support the sectors listed in Annexes I and II to Directive (EU) 2022/2555 and the implementation of Regulation (EU) 2024/2847. To this end, ENISA should also cooperate, where appropriate, with other relevant Union entities.	(34) In order to enhance the shared situational awareness of the cyber threat and incident landscape among stakeholders, ENISA should analyse trends in cyber threats and incidents. This should include a regular analysis addressing the sectors of high criticality and other critical sectors listed in Annexes I and II to Directive (EU) 2022/2555, including the healthcare, energy and transport sectors. Such analysis should include maturity levels of sectors and identify, among others, possible challenges specific to a given sector. Where relevant, and in order to identify supply chain effects, the analysis should evidence cyber threats and trends related to product categories covered by Regulation (EU) 2024/2847. ENISA should develop expertise in the field of cybersecurity of infrastructures and their critical supply chain dependencies, in particular to support the sectors listed in Annexes I and II to Directive (EU) 2022/2555 and the implementation of Regulation (EU) 2024/2847. To this end, ENISA should also cooperate, where appropriate, with other relevant Union entities.
Recital 35		
48	(35) Further, to understand better the challenges in the area of cybersecurity, ENISA needs to analyse current and emerging technologies and provide topic-specific assessments on the expected societal, legal, economic and regulatory impact of technological innovations on cybersecurity. In order to ensure easier access of the public to information on cybersecurity risks and possible remedies, ENISA may provide relevant information on its website, in a user-friendly and well-structured manner.	(35) Further, to understand better the challenges in the area of cybersecurity, ENISA needs to analyse current and emerging technologies and provide topic-specific assessments on the expected societal, legal, economic and regulatory impact of technological innovations on cybersecurity. In order to ensure easier access of the public to information on cybersecurity risks and possible remedies, ENISA may provide relevant information on its website, in a user-friendly and well-structured manner.
Recital 36		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
49	(36) ENISA's strengthened role in fostering situational awareness, analysing threats and providing technical advice will contribute to enhance collective cybersecurity efforts concerning products with digital elements and support the implementation of Regulation (EU) 2024/2847. In accordance with Regulation (EU) 2024/2847, ENISA may propose joint activities to market surveillance authorities for checking compliance of products with digital elements and identify categories of products with digital elements for which sweeps may be organised. Information stemming from cyber threat analysis and early alerts should strengthen the support that ENISA provides to those authorities and contribute to an effective enforcement of Regulation (EU) 2024/2847 to prevent supply chain effects of cyber attacks across the internal market and enhance the overall Union's preparedness.	(36) ENISA's strengthened role in fostering situational awareness, analysing threats and providing technical advice will contribute to enhance collective cybersecurity efforts concerning products with digital elements and support the implementation of Regulation (EU) 2024/2847. In accordance with Regulation (EU) 2024/2847, ENISA may propose joint activities to market surveillance authorities for checking compliance of products with digital elements and identify categories of products with digital elements for which sweeps may be organised. Information stemming from cyber threat analysis and early alerts should strengthen the support that ENISA provides to those authorities and contribute to an effective enforcement of Regulation (EU) 2024/2847 to prevent supply chain effects of cyber attacks across the internal market and enhance the overall Union's preparedness.
Recital 37		
50	(37) Ransomware attacks are a prominent cybersecurity threat to the Union. To boost the Union's cybersecurity and combat ransomware, ENISA should develop capabilities for situational awareness and support for incident response and recovery. When assisting individual essential and important entities in responding to and recovering from a ransomware attack, ENISA should closely cooperate with Europol and with CSIRTs or competent authorities as applicable, thereby drawing from Europol's established experience in fighting ransomware crime. Such assistance should complement CSIRTs' activities supporting incident response. To achieve synergies in its work against ransomware, ENISA should establish a helpdesk and, for that purpose, it could pool relevant capabilities and counter-ransomware services and make easily available information, guidance, and tools that can help essential and important entities respond to and recover from a ransomware incident.	(37) Ransomware attacks are a prominent cybersecurity threat to the Union. To boost the Union's cybersecurity and combat ransomware, ENISA should develop capabilities for situational awareness and support for incident response and recovery. When assisting individual essential and important entities in responding to and recovering from a ransomware attack, ENISA should closely cooperate with Europol and with CSIRTs or competent authorities as applicable, thereby drawing from Europol's established experience in fighting ransomware crime. Such assistance should complement CSIRTs' activities supporting incident response. To achieve synergies in its work against ransomware, ENISA should establish a helpdesk and, for that purpose, it could pool relevant capabilities and counter-ransomware services and make easily available information, guidance, and tools that can help essential and important entities respond to and recover from a ransomware incident.
Recital 38		
51	(38) ENISA should provide technical expertise and support to the Commission in preparing an annual rolling programme of Union-level cybersecurity exercises	(38) ENISA should provide technical expertise and support to the Commission in preparing an annual rolling programme of Union-level cybersecurity exercises

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	in accordance with the Recommendation on the Cyber Blueprint to prepare for cyber crises, to test the level of cybersecurity of entities participating in such exercises, and to minimise duplication of effort. ENISA should, for example, advise on the appropriate types of exercise, such as tabletop, hybrid or full live, as well as objectives, scenarios and participation.	in accordance with the Recommendation on the Cyber Blueprint to prepare for cyber crises, to test the level of cybersecurity of entities participating in such exercises, and to minimise duplication of effort. ENISA should, for example, advise on the appropriate types of exercise, such as tabletop, hybrid or full live, as well as objectives, scenarios and participation.
Recital 39		
52	(39) Access to correct and timely information about vulnerabilities and a robust vulnerability management are imperative for ensuring a high level of cybersecurity in the internal market. For that reason, ENISA should maintain a European vulnerability database pursuant to Directive (EU) 2022/2555 and create a common Union vulnerability management service capacity, ensuring a resilient and sustainable service level and reducing the risk of disruptions. To that end, ENISA should explore possibilities to deepen structured cooperation with programmes, registries or databases similar to the European vulnerability database, in order to avoid a duplication of efforts and to seek complementarity on an international level, where appropriate. Furthermore, ENISA should support multi-party coordinated vulnerability disclosure at Union level and provide value added services, such as vulnerability advisories, severity scoring and product lists, as well as providing an enhanced European known exploited vulnerabilities catalogue to help entities in their vulnerability management.	(39) Access to correct and timely information about vulnerabilities and a robust vulnerability management are imperative for ensuring a high level of cybersecurity in the internal market. For that reason, ENISA should maintain a European vulnerability database pursuant to Directive (EU) 2022/2555 and create a common Union vulnerability management service capacity, ensuring a resilient and sustainable service level and reducing the risk of disruptions. To that end, ENISA should explore possibilities to deepen structured cooperation with programmes, registries or databases similar to the European vulnerability database, in order to avoid a duplication of efforts and to seek complementarity on an international level, where appropriate. Furthermore, ENISA should support multi-party coordinated vulnerability disclosure at Union level and provide value added services, such as vulnerability advisories, severity scoring and product lists, as well as providing an enhanced European known exploited vulnerabilities catalogue to help entities in their vulnerability management.
Recital 40		
53	(40) The role of ENISA in the development of the ECCF should be a key aspect of its mandate. ENISA should provide its technical expertise throughout the lifecycle of European cybersecurity certification schemes. In view of a future scheme, ENISA should identify existing standards or technical specifications that can underlie such as a scheme and, where relevant, draft technical specifications itself that can be referenced in a scheme. ENISA should be in charge of preparing candidate scheme following a Commission request. For schemes already in place, ENISA should be responsible for their maintenance. In	(40) The role of ENISA in the development of the ECCF should be a key aspect of its mandate. ENISA should provide its technical expertise throughout the lifecycle of European cybersecurity certification schemes. In view of a future scheme, ENISA should identify existing standards or technical specifications that can underlie such as a scheme and, where relevant, draft technical specifications itself that can be referenced in a scheme. ENISA should be in charge of preparing candidate scheme following a Commission request. For schemes already in place, ENISA should be responsible for their maintenance. In

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	doing so, ENISA should contribute to building and developing a certification ecosystem where the feedback of Member States and private stakeholders is sought and their certification capacities are reinforced. This should also include operating a dedicated certification website where relevant information related to adopted schemes, including certificates and statements of conformity, is freely and publicly accessible.	doing so, ENISA should contribute to building and developing a certification ecosystem where the feedback of Member States and private stakeholders is sought and their certification capacities are reinforced. This should also include operating a dedicated certification website where relevant information related to adopted schemes, including certificates and statements of conformity, is freely and publicly accessible.
Recital 41		
54	(41) To support the implementation of relevant Union legislation, ENISA should shape the state of the art in cybersecurity by delivering technical specifications to support the implementation of relevant Union legislation, including in view of their potential referencing in European cybersecurity certification schemes. ENISA should also monitor the creation and evolution of standards by relevant standardisation bodies with a view to following standardisation trends at European and global level, and whenever needed, shape such standards by participating to, including through drafting contributions, and leading in the activities of standardisation organisations. In doing so, ENISA should remain impartial. For instance, there might be situations, where ENISA should withdraw from relevant activities in standardisation bodies if ENISA is asked to assess European standards that were requested by the Commission in support of Union legislation. ENISA should not contribute to the drafting of the standards that it is in charge of assessing.	(41) To support the implementation of relevant Union legislation, ENISA should shape the state of the art in cybersecurity by delivering technical specifications to support the implementation of relevant Union legislation, including in view of their potential referencing in European cybersecurity certification schemes. ENISA should also monitor the creation and evolution of standards by relevant standardisation bodies with a view to following standardisation trends at European and global level, and whenever needed, shape such standards by participating to, including through drafting contributions, and leading in the activities of standardisation organisations. In doing so, ENISA should remain impartial. For instance, there might be situations, where ENISA should withdraw from relevant activities in standardisation bodies if ENISA is asked to assess European standards that were requested by the Commission in support of Union legislation. ENISA should not contribute to the drafting of the standards that it is in charge of assessing.
Recital 42		
55	(42) To support the implementation of Union policies and preparation of potential standardisation activities, ENISA should contribute to the development and evaluation of cryptographic algorithms, in particular in the area of post-quantum cryptography. In that context, upon request by the Commission and subject to a contribution agreement as defined in Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council[1], ENISA may establish a process to solicit and evaluate algorithms for cryptographic algorithms	(42) To support the implementation of Union policies and preparation of potential standardisation activities, ENISA should contribute to the development and evaluation of cryptographic algorithms, in particular in the area of post-quantum cryptography. In that context, upon request by the Commission and subject to a contribution agreement as defined in Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council[1], ENISA may establish a process to solicit and evaluate algorithms for cryptographic algorithms

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	by relevant stakeholders, in particular the cryptographic, academic and research communities, as well as manufacturers, CSIRTs, national cybersecurity certification authorities and competent authorities pursuant to Directive (EU) 2022/2555. Where ENISA contributes to establishing such processes, it should promote collaboration between the relevant stakeholders and implement the organisational aspects. The process should be formal, open, transparent and inclusive, including consultation of relevant stakeholders on draft minimum requirements and the evaluation process and evaluation criteria, notably for security and performance of evaluations. _____ 1. Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (OJ L, 2024/2509, 26.09.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).	by relevant stakeholders, in particular the cryptographic, academic and research communities, as well as manufacturers, CSIRTs, national cybersecurity certification authorities and competent authorities pursuant to Directive (EU) 2022/2555. Where ENISA contributes to establishing such processes, it should promote collaboration between the relevant stakeholders and implement the organisational aspects. The process should be formal, open, transparent and inclusive, including consultation of relevant stakeholders on draft minimum requirements and the evaluation process and evaluation criteria, notably for security and performance of evaluations. _____ 1. Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (OJ L, 2024/2509, 26.09.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).
Recital 43		
56	(43) To support the implementation of conformity assessment activities under European cybersecurity certification schemes and other relevant Union legislation, ENISA may provide relevant technical testing tools to support Member States, businesses and conformity assessment bodies in evaluation activities. Such tools should aim to create synergies at Union level and an efficient operation of conformity assessment procedures to meet the needs of Member States and market needs. Such needs may arise for instance in the area of security by design to support businesses, including small and medium-sized enterprises, in their implementation efforts in the context of Regulation 2024/2847. In this context, ENISA should levy fees to cover relevant costs related to establishing, designing, developing, maintaining and updating needed software and hardware capabilities for such testing tools.	(43) To support the implementation of conformity assessment activities under European cybersecurity certification schemes and other relevant Union legislation, ENISA may provide relevant technical testing tools to support Member States, businesses and conformity assessment bodies in evaluation activities. Such tools should aim to create synergies at Union level and an efficient operation of conformity assessment procedures to meet the needs of Member States and market needs. Such needs may arise for instance in the area of security by design to support businesses, including small and medium-sized enterprises, in their implementation efforts in the context of Regulation 2024/2847. In this context, ENISA should levy fees to cover relevant costs related to establishing, designing, developing, maintaining and updating needed software and hardware capabilities for such testing tools.
Recital 44		
57	(44) To support Member States in their efforts to address the shortage of cybersecurity professionals and the growing need for a skilled, diverse, including	(44) To support Member States in their efforts to address the shortage of cybersecurity professionals and the growing need for a skilled, diverse, including

	CLEAN Commission Proposal	VS.EC Council Mandate
	with regards to gender balance, and agile workforce, and to enable labour mobility and preparedness across Member States, ENISA should build on the principles and work initiated under the Cybersecurity Skills Academy. In particular, ENISA should establish the European Cybersecurity Skills Framework ('ECSF') as a common framework on cybersecurity professional role profiles. ENISA should further support Member States in addressing gender disparities in cybersecurity roles. This approach is consistent with the vision outlined in the Commission Communication on the Union of Skills and would contribute to its objectives. A quality label for European individual cybersecurity skills attestations should further be explored.	with regards to gender balance, and agile workforce, and to enable labour mobility and preparedness across Member States, ENISA should build on the principles and work initiated under the Cybersecurity Skills Academy. In particular, ENISA should establish the European Cybersecurity Skills Framework ('ECSF') as a common framework on cybersecurity professional role profiles. ENISA should further support Member States in addressing gender disparities in cybersecurity roles. This approach is consistent with the vision outlined in the Commission Communication on the Union of Skills and would contribute to its objectives. A quality label for European individual cybersecurity skills attestations should further be explored.
Recital 45		
58	(45) The ECSF should be a practical and flexible tool to be used on a voluntary basis that provides a common understanding and terminology of the relevant roles and associated tasks, skills and knowledge mostly required in cybersecurity roles, with a view to supporting the identification of critical skill sets, including transversal skills, required for the workforce, and enabling learning providers, including companies, higher education institutions or vocational education and training providers, to design programmes, and help policymakers to develop initiatives to address skills gaps. Having the potential to be used as a reference framework for skills recognition, it should also be interoperable with the European classification of skills and occupations (ESCO) in order to support human resources departments to understand the requirements for resource planning, recruitment, and career development in support of cybersecurity needs. Whereas DigComp 3.0 describes knowledge, skills and attitudes that are needed to be digitally competent for daily life, participation in society, working and learning, and can be used by both adults and children, the ECSF offer a simple framework identifying cybersecurity roles and associated tasks, knowledge, skills needed to perform them. In this regard, it addresses a specialised audience in cybersecurity, ranging from actually or potential	(45) The ECSF should be a practical and flexible tool to be used on a voluntary basis that provides a common understanding and terminology of the relevant roles and associated tasks, skills and knowledge mostly required in cybersecurity roles, with a view to supporting the identification of critical skill sets, including transversal skills, required for the workforce, and enabling learning providers, including companies, higher education institutions or vocational education and training providers, to design programmes, and help policymakers to develop initiatives to address skills gaps. Having the potential to be used as a reference framework for skills recognition, it should also be interoperable with the European classification of skills and occupations (ESCO) in order to support human resources departments to understand the requirements for resource planning, recruitment, and career development in support of cybersecurity needs. Whereas DigComp 3.0 describes knowledge, skills and attitudes that are needed to be digitally competent for daily life, participation in society, working and learning, and can be used by both adults and children, the ECSF offer a simple framework identifying cybersecurity roles and associated tasks, knowledge, skills needed to perform them. In this regard, it addresses a specialised audience in cybersecurity, ranging from actually or potential

	CLEAN Commission Proposal	VS.EC Council Mandate
	cybersecurity professionals, education institutions to employers. The ECSF should also support the development of European individual cybersecurity skills attestations by being the key instrument used to develop the schemes, allowing the emergence of new market players and supporting market competition within a common framework. The ECSF should be evaluated and updated on a regular basis to ensure that it adequately reflects the cybersecurity labour market's needs, technological and policy developments. ENISA should support the uptake of the ECSF by and within Member States and Union entities, and provide adequate support where such assistance is required.	cybersecurity professionals, education institutions to employers. The ECSF should also support the development of European individual cybersecurity skills attestations by being the key instrument used to develop the schemes, allowing the emergence of new market players and supporting market competition within a common framework. The ECSF should be evaluated and updated on a regular basis to ensure that it adequately reflects the cybersecurity labour market's needs, technological and policy developments. ENISA should support the uptake of the ECSF by and within Member States and Union entities, and provide adequate support where such assistance is required.
Recital 46		
59	(46) Cybersecurity skills and qualifications should be made comparable, transparent and trusted across the internal market. To this end, European individual cybersecurity skills attestations[1] should support employers, including SMEs and startups, to recruit actual or potential cybersecurity professionals in an effective manner within and across Member States, in line with the objectives set out in the Communication on the Union of Skills. To ensure consistent implementation across Member States, European individual cybersecurity skills attestations should be based on a common understanding, at Union level, of the skills needed to meet those objectives and should be delivered by providers authorised by ENISA against a common set of criteria. This approach should be consistent with and contribute to the objectives of the future Skills Portability Initiative. _____ 1. European individual cybersecurity skills attestations should be understood as following a similar approach to what the market recognises as 'cybersecurity certifications'. However, in order to avoid confusion with regards to the European Cybersecurity Certification Framework, the expression 'attestation', already used in the communication on the Cybersecurity Skills Academy, is preferred.	(46) Cybersecurity skills and qualifications should be made comparable, transparent and trusted across the internal market. To this end, European individual cybersecurity skills attestations[1] should support employers, including SMEs and startups, to recruit actual or potential cybersecurity professionals in an effective manner within and across Member States, in line with the objectives set out in the Communication on the Union of Skills. To ensure consistent implementation across Member States, European individual cybersecurity skills attestations should be based on a common understanding, at Union level, of the skills needed to meet those objectives and should be delivered by providers authorised by ENISA against a common set of criteria. This approach should be consistent with and contribute to the objectives of the future Skills Portability Initiative. _____ 1. European individual cybersecurity skills attestations should be understood as following a similar approach to what the market recognises as 'cybersecurity certifications'. However, in order to avoid confusion with regards to the European Cybersecurity Certification Framework, the expression 'attestation', already used in the communication on the Cybersecurity Skills Academy, is preferred.
Recital 47		
60	(47) The development of European individual cybersecurity skills attestation	(47) The development of European individual cybersecurity skills attestation

	CLEAN Commission Proposal	VS.EC Council Mandate
	schemes should aim to supplement Member States' actions by offering the possibility to public authorities and economic actors to make use of a European attestation mechanism, in line with the supporting competence of the Union in the area of education and vocational training, as referred to in Article 6, point (e) and Articles 165(1) and 166(1) TFEU. The schemes, together with the work of the Cybersecurity Skills Academy, can also represent the basis for the higher education programmes, such as sectoral European degrees and for the development of micro-credentials. Therefore, the European individual cybersecurity attestation schemes should not aim to harmonise law and regulations in Member States, but rather be considered as an enabler and an opportunity which Member States and economic actors may wish to take up and promote.	schemes should aim to supplement Member States' actions by offering the possibility to public authorities and economic actors to make use of a European attestation mechanism, in line with the supporting competence of the Union in the area of education and vocational training, as referred to in Article 6, point (e) and Articles 165(1) and 166(1) TFEU. The schemes, together with the work of the Cybersecurity Skills Academy, can also represent the basis for the higher education programmes, such as sectoral European degrees and for the development of micro-credentials. Therefore, the European individual cybersecurity attestation schemes should not aim to harmonise law and regulations in Member States, but rather be considered as an enabler and an opportunity which Member States and economic actors may wish to take up and promote.
Recital 48		
61	(48) ENISA should ensure that European individual cybersecurity skills attestation schemes remain close to market needs and build on experience from both public and private providers of individual certifications, including Member States, higher education institutions, vocational education and training institutions and businesses. ENISA should consult the Commission on prioritisation of the European individual cybersecurity skills attestation schemes, taking into due consideration policy implementation and market needs.	(48) ENISA should ensure that European individual cybersecurity skills attestation schemes remain close to market needs and build on experience from both public and private providers of individual certifications, including Member States, higher education institutions, vocational education and training institutions and businesses. ENISA should consult the Commission on prioritisation of the European individual cybersecurity skills attestation schemes, taking into due consideration policy implementation and market needs.
Recital 49		
62	(49) To ensure alignment between the ECSF and the schemes, revision of an ECSF role profile should automatically trigger an evaluation of fitness of the associated European individual cybersecurity skills attestation scheme or schemes, which may lead to their review.	(49) To ensure alignment between the ECSF and the schemes, revision of an ECSF role profile should automatically trigger an evaluation of fitness of the associated European individual cybersecurity skills attestation scheme or schemes, which may lead to their review.
Recital 50		
63	(50) Taking into consideration the diversity of cybersecurity role profiles and associated tasks, skills and knowledge, the assessment of individuals and	(50) Taking into consideration the diversity of cybersecurity role profiles and associated tasks, skills and knowledge, the assessment of individuals and

	CLEAN Commission Proposal	VS.EC Council Mandate
	assessment methods may have to be adapted in each European individual cybersecurity skills attestation scheme. Each scheme should ensure that the assessment of an individual's required skills in terms of learning outcomes, including, where relevant, the evaluation of the level of proficiency, is systematically evaluated against an ECSF role profile or subset thereof. Assessment methods may include elements such as testing theoretical knowledge, practical examination, prerequisites and peer assessment. Experience of individuals should be duly taken into consideration.	assessment methods may have to be adapted in each European individual cybersecurity skills attestation scheme. Each scheme should ensure that the assessment of an individual's required skills in terms of learning outcomes, including, where relevant, the evaluation of the level of proficiency, is systematically evaluated against an ECSF role profile or subset thereof. Assessment methods may include elements such as testing theoretical knowledge, practical examination, prerequisites and peer assessment. Experience of individuals should be duly taken into consideration.
Recital 51		
64	(51) In order to ensure a consistent implementation of European individual cybersecurity skills attestation schemes, in particular with regard to the assessment of individuals, ENISA should provide obligatory training to personnel in charge of carrying out the assessment of individuals. Such personnel should have experience in the field of cybersecurity which could be demonstrated by holding a European individual cybersecurity skills attestation for the role profile they are conducting the assessment for and at a proficiency level at least equivalent to that of the individuals they are assessing.	(51) In order to ensure a consistent implementation of European individual cybersecurity skills attestation schemes, in particular with regard to the assessment of individuals, ENISA should provide obligatory training to personnel in charge of carrying out the assessment of individuals. Such personnel should have experience in the field of cybersecurity which could be demonstrated by holding a European individual cybersecurity skills attestation for the role profile they are conducting the assessment for and at a proficiency level at least equivalent to that of the individuals they are assessing.
Recital 52		
65	(52) The role of the authorised attestation providers is to attest the knowledge and competences of an individual to be able to perform one of the ECSF roles and to give assurance to the employers across the Union. As also employers operating Unions critical infrastructure would look at the assurance of the quality of skills and competences of individuals acquiring European individual cybersecurity skills attestation, the authorised providers attesting the level of skills and competences should be trustworthy from the cybersecurity point of view and should not be subject of the undue influence by a third country that may pose cybersecurity concerns. Therefore, entities established in a third country posing cybersecurity concerns designated in accordance with this Regulation or controlled by such third country, by an entity established in such	(52) The role of the authorised attestation providers is to attest the knowledge and competences of an individual to be able to perform one of the ECSF roles and to give assurance to the employers across the Union. As also employers operating Unions critical infrastructure would look at the assurance of the quality of skills and competences of individuals acquiring European individual cybersecurity skills attestation, the authorised providers attesting the level of skills and competences should be trustworthy from the cybersecurity point of view and should not be subject of the undue influence by a third country that may pose cybersecurity concerns. Therefore, entities established in a third country posing cybersecurity concerns designated in accordance with this Regulation or controlled by such third country, by an entity established in such

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	third country, or by a national of such third country (high-risk suppliers) in accordance with this Regulation should not be eligible to become authorised attestation providers of any European individual cybersecurity skills attestations pursuant to Title II, Section 4.	third country, or by a national of such third country (high-risk suppliers) in accordance with this Regulation should not be eligible to become authorised attestation providers of any European individual cybersecurity skills attestations pursuant to Title II, Section 4.
Recital 53		
66	(53) To ensure that individuals that hold a European cybersecurity skills attestation can easily use and share it, and that such an attestation can be used across Member States, authorised attestation providers should ensure that electronic attestations of the European individual cybersecurity skills attestations are issued to the European Digital Identity Wallet (EUDI wallet) established by Regulation (EU) No 910/2014 at the request of the individual. Authorised attestation providers should be considered as trust service providers and subject to the supervisory and liability regime laid down in Regulation (EU) No 910/2014. The scheme for the attestation of attributes used pursuant to Commission Implementing Regulation (EU) 2025/1569[1] should be registered in the catalogue of schemes for the attestation of attributes provided for in that Implementing Regulation. _____ 1. Implementing regulation - EU - 2025/1569	(53) To ensure that individuals that hold a European cybersecurity skills attestation can easily use and share it, and that such an attestation can be used across Member States, authorised attestation providers should ensure that electronic attestations of the European individual cybersecurity skills attestations are issued to the European Digital Identity Wallet (EUDI wallet) established by Regulation (EU) No 910/2014 at the request of the individual. Authorised attestation providers should be considered as trust service providers and subject to the supervisory and liability regime laid down in Regulation (EU) No 910/2014. The scheme for the attestation of attributes used pursuant to Commission Implementing Regulation (EU) 2025/1569[1] should be registered in the catalogue of schemes for the attestation of attributes provided for in that Implementing Regulation. _____ 1. Implementing regulation - EU - 2025/1569
Recital 54		
67	(54) To contribute to the development of the cybersecurity workforce and the portability of skills across the Union, ENISA should make the European individual cybersecurity skills attestation schemes and the list of authorised attestation providers available to the public via a dedicated website.	(54) To contribute to the development of the cybersecurity workforce and the portability of skills across the Union, ENISA should make the European individual cybersecurity skills attestation schemes and the list of authorised attestation providers available to the public via a dedicated website.
Recital 55		
68	(55) ENISA should be governed and operated taking into account the principles of the Common Approach on Union decentralised agencies adopted on 19 July 2012 by the European Parliament, the Council and the Commission[1].	(55) ENISA should be governed and operated taking into account the principles of the Common Approach on Union decentralised agencies adopted on 19 July 2012 by the European Parliament, the Council and the Commission[1].

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	The recommendations in the Common Approach should also be reflected, as appropriate, in ENISA's work programmes, evaluations of ENISA, and ENISA's reporting and administrative practice. _____ 1. Common Approach, annexed to the Joint Statement of the European Parliament, the Council of the EU and the European Commission on decentralised agencies, adopted on 19 July 2012 and available at: https://european-union.europa.eu/document/download/d4199ff4-1e3d-45e6-af7e-90cf1a7b10bc_en?filename=joint_statement_on_decentralised_agencies_en.pdf.	The recommendations in the Common Approach should also be reflected, as appropriate, in ENISA's work programmes, evaluations of ENISA, and ENISA's reporting and administrative practice. _____ 1. Common Approach, annexed to the Joint Statement of the European Parliament, the Council of the EU and the European Commission on decentralised agencies, adopted on 19 July 2012 and available at: https://european-union.europa.eu/document/download/d4199ff4-1e3d-45e6-af7e-90cf1a7b10bc_en?filename=joint_statement_on_decentralised_agencies_en.pdf.
Recital 56		
69	(56) In order for the Management Board to perform its functions effectively, particularly in guiding the overall direction of ENISA's activities and setting its strategic priorities, it is essential for the Board to consist of high-level representatives from Member States and the Commission. To that end, each Member State should appoint the head of a national competent authority of that Member State responsible for cybersecurity designated pursuant to Article 8(1) of Directive (EU) 2022/2555 as a member of the Management Board.	(56) In order for the Management Board to perform its functions effectively, particularly in guiding the overall direction of ENISA's activities and setting its strategic priorities, it is essential for the Board to consist of high-level representatives from Member States and the Commission. To that end, each Member State should appoint the head of a national competent authority of that Member State responsible for cybersecurity designated pursuant to Article 8(1) of Directive (EU) 2022/2555 as a member of the Management Board.
Recital 57		
70	(57) To ensure that alternates in the Management Board can fulfil their roles adequately, Member States should appoint alternates that have appropriate professional expertise and experience. The Commission and the Member States, as regards alternates, should make efforts to achieve a balanced representation between men and women on the Management Board and should limit their turnover in order to ensure continuity of the Management Board's work.	(57) To ensure that alternates in the Management Board can fulfil their roles adequately, Member States should appoint alternates that have appropriate professional expertise and experience. The Commission and the Member States, as regards alternates, should make efforts to achieve a balanced representation between men and women on the Management Board and should limit their turnover in order to ensure continuity of the Management Board's work.
Recital 58		
71	(58) To enable ENISA to fulfil its mission effectively, the Management Board, composed of the representatives of the Member States and of the Commission, should establish the general direction of ENISA's operations, including its strategic priorities, and ensure that it carries out its tasks in accordance with this Regulation. The Management Board should be entrusted with the powers	(58) To enable ENISA to fulfil its mission effectively, the Management Board, composed of the representatives of the Member States and of the Commission, should establish the general direction of ENISA's operations, including its strategic priorities, and ensure that it carries out its tasks in accordance with this Regulation. The Management Board should be entrusted with the powers

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	necessary to establish and verify the execution of the budget, adopt appropriate financial rules, establish transparent working procedures for decision making by ENISA, adopt ENISA's single programming document, adopt its own rules of procedure, appoint the Executive Director, decide on the extension and termination of the Executive Director's term of office, and decide whether to create a function of Deputy Executive Director and, if such a function is created, on their appointment, and the extension and termination of their term of office. Any person exercising an executive function within ENISA should therefore be appointed by the Management Board. The Management Board should also be responsible for appointing or dismissing members of the Board of Appeal, as well as establishing rules to prevent or manage conflicts of interest in this respect.	necessary to establish and verify the execution of the budget, adopt appropriate financial rules, establish transparent working procedures for decision making by ENISA, adopt ENISA's single programming document, adopt its own rules of procedure, appoint the Executive Director, decide on the extension and termination of the Executive Director's term of office, and decide whether to create a function of Deputy Executive Director and, if such a function is created, on their appointment, and the extension and termination of their term of office. Any person exercising an executive function within ENISA should therefore be appointed by the Management Board. The Management Board should also be responsible for appointing or dismissing members of the Board of Appeal, as well as establishing rules to prevent or manage conflicts of interest in this respect.
Recital 59		
72	(59) To help ensure that ENISA establishes its strategic priorities and maintains them up to date, the Management Board should hold at least one meeting per year dedicated to the strategic priorities of ENISA. To ensure that meetings of the Management Board are effective and well-informed, the Management Board may invite to its meetings any person whose opinion could be pertinent and of interest to the topics discussed to provide insights, expertise or advice. Such a person would be an ad hoc observer without voting rights.	(59) To help ensure that ENISA establishes its strategic priorities and maintains them up to date, the Management Board should hold at least one meeting per year dedicated to the strategic priorities of ENISA. To ensure that meetings of the Management Board are effective and well-informed, the Management Board may invite to its meetings any person whose opinion could be pertinent and of interest to the topics discussed to provide insights, expertise or advice. Such a person would be an ad hoc observer without voting rights.
Recital 60		
73	(60) The Management Board should adopt decisions by an absolute majority of its members with voting rights, unless otherwise provided for in this Regulation. Due to the importance of budgetary and human resources matters, in particular matters on the annual budget, annual activity report, the anti-fraud strategy, implementing rules giving effect to Staff Regulations, the appointment of the Executive Director, the Deputy Executive Director and the accounting officer, follow-up to findings of the European Anti-Fraud Office (OLAF) and of the European Public Prosecutor's Office (EPPO), and the adoption of the financial rules of ENISA, the Management Board should adopt such decisions only if the	(60) The Management Board should adopt decisions by an absolute majority of its members with voting rights, unless otherwise provided for in this Regulation. Due to the importance of budgetary and human resources matters, in particular matters on the annual budget, annual activity report, the anti-fraud strategy, implementing rules giving effect to Staff Regulations, the appointment of the Executive Director, the Deputy Executive Director and the accounting officer, follow-up to findings of the European Anti-Fraud Office (OLAF) and of the European Public Prosecutor's Office (EPPO), and the adoption of the financial rules of ENISA, the Management Board should adopt such decisions only if the

	CLEAN Commission Proposal	VS.EC Council Mandate
	representative of the Commission casts a positive vote. For the purposes of taking a decision on adopting a final single programming document after taking into account Commission's opinion, a positive vote of the representative of the Commission should only be required on the elements of the decision not related to the annual and multiannual work programme of ENISA.	representative of the Commission casts a positive vote. For the purposes of taking a decision on adopting a final single programming document after taking into account Commission's opinion, a positive vote of the representative of the Commission should only be required on the elements of the decision not related to the annual and multiannual work programme of ENISA.
Recital 61		
74	(61) The Executive Board should contribute to the effective functioning of the Management Board. As part of its preparatory work related to Management Board decisions, the Executive Board should examine relevant information in detail, explore available options and offer advice and solutions to prepare the decisions of the Management Board. It should also assist and advise the Executive Director in implementing Management Board decisions.	(61) The Executive Board should contribute to the effective functioning of the Management Board. As part of its preparatory work related to Management Board decisions, the Executive Board should examine relevant information in detail, explore available options and offer advice and solutions to prepare the decisions of the Management Board. It should also assist and advise the Executive Director in implementing Management Board decisions.
Recital 62		
75	(62) The smooth functioning of ENISA requires that its Executive Director be appointed on grounds of merit and documented administrative and managerial skills, as well as competence and experience relevant to cybersecurity. The duties of the Executive Director should be carried out with complete independence. The Management Board should appoint the Executive Director from the list of candidates prepared by the Commission, following an open and transparent procedure that respects the principle of gender balance.	(62) The smooth functioning of ENISA requires that its Executive Director be appointed on grounds of merit and documented administrative and managerial skills, as well as competence and experience relevant to cybersecurity. The duties of the Executive Director should be carried out with complete independence. The Management Board should appoint the Executive Director from the list of candidates prepared by the Commission, following an open and transparent procedure that respects the principle of gender balance.
Recital 63		
76	(63) The Executive Director should prepare a proposal for ENISA's single programming document, after prior consultation with the Commission, and should take all steps necessary to ensure the proper implementation of that single programming document. The Executive Director should prepare an annual report to be submitted to the Management Board, covering the implementation of ENISA's annual work programme, draw up a draft statement of estimates of revenue and expenditure for ENISA, and implement the budget. Furthermore,	(63) The Executive Director should prepare a proposal for ENISA's single programming document, after prior consultation with the Commission, and should take all steps necessary to ensure the proper implementation of that single programming document. The Executive Director should prepare an annual report to be submitted to the Management Board, covering the implementation of ENISA's annual work programme, draw up a draft statement of estimates of revenue and expenditure for ENISA, and implement the budget. Furthermore,

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	the Executive Director should have the option of setting up ad hoc working groups to address specific matters, in particular matters of a scientific, technical, legal or socio-economic nature. In particular, in relation to the preparation of a specific candidate European cybersecurity certification scheme ('candidate scheme'), the setting up of an ad hoc working group is considered to be necessary. Setting up of an ad hoc working group might also be necessary for maintenance activities in relation to specific adopted European cybersecurity certification schemes. Ad hoc working groups should also be set up to develop and maintain European individual cybersecurity skills attestation schemes and assist the Agency in the governance, implementation and evolution of the ECSF. The Executive Director should ensure that the members of ad hoc working groups are selected according to the highest standards of expertise, aiming to ensure gender balance and an appropriate balance, according to the specific issues in question, between the public administrations of the Member States, the Union entities and the private sector, including industry, users, and academic experts in network and information security, as well as academic experts in products with digital elements.	the Executive Director should have the option of setting up ad hoc working groups to address specific matters, in particular matters of a scientific, technical, legal or socio-economic nature. In particular, in relation to the preparation of a specific candidate European cybersecurity certification scheme ('candidate scheme'), the setting up of an ad hoc working group is considered to be necessary. Setting up of an ad hoc working group might also be necessary for maintenance activities in relation to specific adopted European cybersecurity certification schemes. Ad hoc working groups should also be set up to develop and maintain European individual cybersecurity skills attestation schemes and assist the Agency in the governance, implementation and evolution of the ECSF. The Executive Director should ensure that the members of ad hoc working groups are selected according to the highest standards of expertise, aiming to ensure gender balance and an appropriate balance, according to the specific issues in question, between the public administrations of the Member States, the Union entities and the private sector, including industry, users, and academic experts in network and information security, as well as academic experts in products with digital elements.
Recital 64		
77	(64) The Management Board may decide to create a function of a Deputy Executive Director to assist the Executive Director, where the Management Board considers that such a function is necessary to ensure or maintain the smooth functioning of ENISA. When deciding on whether to create that function, the Management Board may take into account the opinion of the Executive Director.	(64) The Management Board may decide to create a function of a Deputy Executive Director to assist the Executive Director, where the Management Board considers that such a function is necessary to ensure or maintain the smooth functioning of ENISA. When deciding on whether to create that function, the Management Board may take into account the opinion of the Executive Director.
Recital 65		
78	(65) ENISA should have an Advisory Group to ensure regular dialogue with the private sector, consumers' organisations and other relevant stakeholders. The ENISA Advisory Group, established by the Management Board on a proposal from the Executive Director, should focus on issues relevant to stakeholders and	(65) ENISA should have an Advisory Group to ensure regular dialogue with the private sector, consumers' organisations and other relevant stakeholders. The ENISA Advisory Group, established by the Management Board on a proposal from the Executive Director, should focus on issues relevant to stakeholders and

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	should bring them to the attention of ENISA. The ENISA Advisory Group should be consulted in particular with regard to ENISA's draft annual work programme. The composition of the ENISA Advisory Group and the tasks assigned to it should ensure sufficient representation of stakeholders in the work of ENISA. Representatives of national and Union law enforcement, data protection and market surveillance authorities should be eligible to be represented in the ENISA Advisory Group.	should bring them to the attention of ENISA. The ENISA Advisory Group should be consulted in particular with regard to ENISA's draft annual work programme. The composition of the ENISA Advisory Group and the tasks assigned to it should ensure sufficient representation of stakeholders in the work of ENISA. Representatives of national and Union law enforcement, data protection and market surveillance authorities should be eligible to be represented in the ENISA Advisory Group.
Recital 66		
79	(66) Applicants to become authorised attestation providers or to renew their authorisation should have access to the necessary remedies where they are affected by decisions taken by ENISA. Therefore, an appropriate appeal mechanism should be set up so that related decisions of ENISA can be challenged before a Board of Appeal, the decisions of which can be subject to judicial review by the Court of Justice of the European Union in accordance with the Treaties. The requirement to exhaust the appeal procedure within ENISA before bringing an action before the Court of Justice of the European Union is only applicable to the persons that have standing before the Board of Appeals.	(66) Applicants to become authorised attestation providers or to renew their authorisation should have access to the necessary remedies where they are affected by decisions taken by ENISA. Therefore, an appropriate appeal mechanism should be set up so that related decisions of ENISA can be challenged before a Board of Appeal, the decisions of which can be subject to judicial review by the Court of Justice of the European Union in accordance with the Treaties. The requirement to exhaust the appeal procedure within ENISA before bringing an action before the Court of Justice of the European Union is only applicable to the persons that have standing before the Board of Appeals.
Recital 67		
80	(67) In order to guarantee the full autonomy and independence of ENISA and to enable it to perform its tasks, ENISA should be granted a sufficient and autonomous budget primarily funded from a contribution from the Union, but also from contributions from third countries participating in ENISA's work, and from fees paid by authorised attestation providers and by conformity assessment bodies participating in schemes and issuing European cybersecurity certificates and EU statements of conformity. The host Member State, and any other Member State, should be allowed to make voluntary contributions to ENISA's budget. No contribution, whether financial or in kind, received by ENISA from Member States, third countries, or other entities or persons should compromise	(67) In order to guarantee the full autonomy and independence of ENISA and to enable it to perform its tasks, ENISA should be granted a sufficient and autonomous budget primarily funded from a contribution from the Union, but also from contributions from third countries participating in ENISA's work, and from fees paid by authorised attestation providers and by conformity assessment bodies participating in schemes and issuing European cybersecurity certificates and EU statements of conformity. The host Member State, and any other Member State, should be allowed to make voluntary contributions to ENISA's budget. No contribution, whether financial or in kind, received by ENISA from Member States, third countries, or other entities or persons should compromise

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	its independence and impartiality. The Union budgetary procedure should be applicable as far as the Union contribution and any other subsidies chargeable to the general budget of the Union are concerned. The Court of Auditors should audit ENISA's accounts to ensure transparency and accountability. In order to enable the Agency to participate in all relevant future projects, it should be given the possibility to receive grants.	its independence and impartiality. The Union budgetary procedure should be applicable as far as the Union contribution and any other subsidies chargeable to the general budget of the Union are concerned. The Court of Auditors should audit ENISA's accounts to ensure transparency and accountability. In order to enable the Agency to participate in all relevant future projects, it should be given the possibility to receive grants.
Recital 68		
81	(68) To ensure ENISA's capacity to respond to demand for the activities it carries out, in particular as regards decisions to authorise providers to deliver European individual cybersecurity skills attestations, and as regards the maintenance of the European cybersecurity certification schemes and of testing tools, ENISA should be given the power to levy fees. Fees associated with processing of applications to become an authorised attestation provider should be appropriately determined to sufficiently contribute to covering the estimated costs of developing and maintaining the European individual cybersecurity skills attestation schemes and evaluating whether requirements and obligations to become and remain an authorised attestation provider are and continue to be met. Fees associated to the costs of issuing and renewing authorisations to authorised attestation providers should include costs associated to evaluations performed by or under the supervision of ENISA. Fees associated with the participation in European cybersecurity certifications schemes and for the issuance of certificates under such schemes should be appropriately determined to sufficiently contribute to covering the estimated costs of maintaining such schemes. The payment of such fees should enable notified conformity assessment bodies and, where applicable, certificate holders under a scheme to take part in such activities as well as relevant capacity building and promotional activities to promote the exchange of best practices and foster the uptake of schemes and certified solutions.	(68) To ensure ENISA's capacity to respond to demand for the activities it carries out, in particular as regards decisions to authorise providers to deliver European individual cybersecurity skills attestations, and as regards the maintenance of the European cybersecurity certification schemes and of testing tools, ENISA should be given the power to levy fees. Fees associated with processing of applications to become an authorised attestation provider should be appropriately determined to sufficiently contribute to covering the estimated costs of developing and maintaining the European individual cybersecurity skills attestation schemes and evaluating whether requirements and obligations to become and remain an authorised attestation provider are and continue to be met. Fees associated to the costs of issuing and renewing authorisations to authorised attestation providers should include costs associated to evaluations performed by or under the supervision of ENISA. Fees associated with the participation in European cybersecurity certifications schemes and for the issuance of certificates under such schemes should be appropriately determined to sufficiently contribute to covering the estimated costs of maintaining such schemes. The payment of such fees should enable notified conformity assessment bodies and, where applicable, certificate holders under a scheme to take part in such activities as well as relevant capacity building and promotional activities to promote the exchange of best practices and foster the uptake of schemes and certified solutions.
Recital 69		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
82	(69) To ensure proportionality, transparency and legal certainty, fees should be set in a transparent and fair manner. All expenditure of ENISA attributed to staff involved in activities subject to fees, in particular the employer's pro-rata contribution to the pension scheme, and costs related to the Board of Appeal, should be reflected in that cost. Fees must not lead to the imposition of unnecessary financial or administrative burdens on applicants. Reasonable deadlines should be set for the payment of fees.	(69) To ensure proportionality, transparency and legal certainty, fees should be set in a transparent and fair manner. All expenditure of ENISA attributed to staff involved in activities subject to fees, in particular the employer's pro-rata contribution to the pension scheme, and costs related to the Board of Appeal, should be reflected in that cost. Fees must not lead to the imposition of unnecessary financial or administrative burdens on applicants. Reasonable deadlines should be set for the payment of fees.
Recital 70		
83	(70) It is necessary to put in place a set of indicators to measure the Agency's workload, effectiveness and efficiency in relation to activities financed through fees. Having regard to these indicators, the Agency should adapt its staff planning and management of resources related to fees to be able to adequately respond to such demand and to any fluctuations in revenue from fees.	(70) It is necessary to put in place a set of indicators to measure the Agency's workload, effectiveness and efficiency in relation to activities financed through fees. Having regard to these indicators, the Agency should adapt its staff planning and management of resources related to fees to be able to adequately respond to such demand and to any fluctuations in revenue from fees.
Recital 71		
84	(71) To identify and correctly manage the risk of actual or perceived conflict of interests, ENISA should have rules in place regarding the prevention and the management of conflicts of interest. ENISA should also apply the rules on access to documents set out in Regulation (EC) No 1049/2001 of the European Parliament and of the Council[1]. The processing of personal data by ENISA should be subject to Regulation (EU) 2018/1725 of the European Parliament and of the Council[2]. ENISA should comply with the provisions applicable to the Union entities, and with national legislation regarding the handling of information, in particular sensitive non-classified information and European Union classified information (EUCI). _____ 1. Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43, ELI: http://data.europa.eu/eli/reg/2001/1049/oj). 2. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union	(71) To identify and correctly manage the risk of actual or perceived conflict of interests, ENISA should have rules in place regarding the prevention and the management of conflicts of interest. ENISA should also apply the rules on access to documents set out in Regulation (EC) No 1049/2001 of the European Parliament and of the Council[1]. The processing of personal data by ENISA should be subject to Regulation (EU) 2018/1725 of the European Parliament and of the Council[2]. ENISA should comply with the provisions applicable to the Union entities, and with national legislation regarding the handling of information, in particular sensitive non-classified information and European Union classified information (EUCI). _____ 1. Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43, ELI: http://data.europa.eu/eli/reg/2001/1049/oj). 2. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).	institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).
Recital 72		
85	(72) When performing its tasks, ENISA may have access to sensitive information, such as information regarding cyber threats and incidents. Therefore, it is essential for ENISA to preserve the confidentiality of information it handles. In particular, in line with Article 339 of the Treaty on the Functioning of the European Union (TFEU), officials and other servants of ENISA should not disclose any information of the kind covered by the obligation of professional secrecy, in particular information about undertakings, their business relations or their cost components, even after their duties have ceased.	(72) When performing its tasks, ENISA may have access to sensitive information, such as information regarding cyber threats and incidents. Therefore, it is essential for ENISA to preserve the confidentiality of information it handles. In particular, in line with Article 339 of the Treaty on the Functioning of the European Union (TFEU), officials and other servants of ENISA should not disclose any information of the kind covered by the obligation of professional secrecy, in particular information about undertakings, their business relations or their cost components, even after their duties have ceased.
Recital 73		
86	(73) To ensure that it fully achieves its objectives, ENISA should liaise with the relevant Union supervisory authorities and with other competent authorities in the Union, relevant Union entities, including CERT-EU, EC3 at Europol, the ECCC, the European Defence Agency (EDA), the European Union Agency for the Space Programme (EUSPA), the Body of European Regulators for Electronic Communications (BEREC), the European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), the European Central Bank (ECB), the European Banking Authority (EBA), the European Data Protection Board, the Agency for the Cooperation of Energy Regulators (ACER), the European Union Aviation Safety Agency (EASA), and any other Union entity involved in cybersecurity. ENISA should also liaise with competent authorities under Directive (EU) 2022/2555, market surveillance authorities and authorities that deal with data protection in order to exchange know-how and best practices and should provide advice on cybersecurity issues that might have an impact on their work.	(73) To ensure that it fully achieves its objectives, ENISA should liaise with the relevant Union supervisory authorities and with other competent authorities in the Union, relevant Union entities, including CERT-EU, EC3 at Europol, the ECCC, the European Defence Agency (EDA), the European Union Agency for the Space Programme (EUSPA), the Body of European Regulators for Electronic Communications (BEREC), the European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), the European Central Bank (ECB), the European Banking Authority (EBA), the European Data Protection Board, the Agency for the Cooperation of Energy Regulators (ACER), the European Union Aviation Safety Agency (EASA), and any other Union entity involved in cybersecurity. ENISA should also liaise with competent authorities under Directive (EU) 2022/2555, market surveillance authorities and authorities that deal with data protection in order to exchange know-how and best practices and should provide advice on cybersecurity issues that might have an impact on their work.
Recital 74		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
87	(74) Europol has an important role in preventing and combating cybercrime, including cybercrime related to network and information security incidents. To create synergies between the respective tasks of each Agency, ENISA should cooperate with Europol, in particular by sharing information regarding trends in techniques, demands and impacts of ransomware attacks. Such cooperation may also consist in identifying the most common ransomware strains targeting entities listed in Annexes I and II to Directive (EU) 2022/2555 to support essential and important entities in incident response and recovery.	(74) Europol has an important role in preventing and combating cybercrime, including cybercrime related to network and information security incidents. To create synergies between the respective tasks of each Agency, ENISA should cooperate with Europol, in particular by sharing information regarding trends in techniques, demands and impacts of ransomware attacks. Such cooperation may also consist in identifying the most common ransomware strains targeting entities listed in Annexes I and II to Directive (EU) 2022/2555 to support essential and important entities in incident response and recovery.
Recital 75		
88	(75) To support operational cooperation and shared situational awareness of cyber threats and incidents, it is essential for ENISA to cooperate with stakeholders and in particular companies and organisations from the private sector, with which ENISA may establish public-private partnerships.	(75) To support operational cooperation and shared situational awareness of cyber threats and incidents, it is essential for ENISA to cooperate with stakeholders and in particular companies and organisations from the private sector, with which ENISA may establish public-private partnerships.
Recital 76		
89	(76) To effectively meet the goals outlined in this Regulation, ENISA may collaborate in particular with academic institutions that have research initiatives in relevant fields, and develop appropriate channels for input from consumer organisations and other organisations.	(76) To effectively meet the goals outlined in this Regulation, ENISA may collaborate in particular with academic institutions that have research initiatives in relevant fields, and develop appropriate channels for input from consumer organisations and other organisations.
Recital 77		
90	(77) Given the borderless nature of cyber threats and incidents, the level of cybersecurity and preparedness of third countries may impact entities in the Union. Therefore, ENISA should be able to provide capacity-building activities, including training, capacity-building, twinning activities in third countries, and in particular tailored capacity-building activities for countries that are candidates for accession to the Union or other partner countries in accordance with the Union priorities. Such activities should be conducted following a specific request to provide adequate support, taking into account the priorities of the Union, and be implemented through special arrangements, including through contribution	(77) Given the borderless nature of cyber threats and incidents, the level of cybersecurity and preparedness of third countries may impact entities in the Union. Therefore, ENISA should be able to provide capacity-building activities, including training, capacity-building, twinning activities in third countries, and in particular tailored capacity-building activities for countries that are candidates for accession to the Union or other partner countries in accordance with the Union priorities. Such activities should be conducted following a specific request to provide adequate support, taking into account the priorities of the Union, and be implemented through special arrangements, including through contribution

	CLEAN Commission Proposal	VS.EC Council Mandate
	agreements as referred to in Regulation (EU, Euratom) 2024/2509. The European cybersecurity certification framework aims to protect against cyber threats such as maliciously exploited cybersecurity vulnerabilities or cybersecurity incidents affecting the functionality (design and operation) of ICT products, ICT services, ICT processes, managed security services, or cyber posture of entities. By focusing on technical risks related to ICT products, ICT services, ICT processes, managed security services or cyber posture of entities, the ECCF should complement the security of ICT supply chains framework, which aims to ensure a harmonised approach at Union level to address non-technical risks in sectors of high criticality and other critical sectors.	agreements as referred to in Regulation (EU, Euratom) 2024/2509. The European cybersecurity certification framework aims to protect against cyber threats such as maliciously exploited cybersecurity vulnerabilities or cybersecurity incidents affecting the functionality (design and operation) of ICT products, ICT services, ICT processes, managed security services, or cyber posture of entities. By focusing on technical risks related to ICT products, ICT services, ICT processes, managed security services or cyber posture of entities, the ECCF should complement the security of ICT supply chains framework, which aims to ensure a harmonised approach at Union level to address non-technical risks in sectors of high criticality and other critical sectors.
Recital 78		
91	(78) It should be possible for Member States to have recourse to European cybersecurity certification in the context of public procurement in accordance with Directive 2014/24/EU of the European Parliament and of the Council[1]. _____ 1. Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, p. 65, ELI: http://data.europa.eu/eli/dir/2014/24/oj).	(78) It should be possible for Member States to have recourse to European cybersecurity certification in the context of public procurement in accordance with Directive 2014/24/EU of the European Parliament and of the Council[1]. _____ 1. Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, p. 65, ELI: http://data.europa.eu/eli/dir/2014/24/oj).
Recital 79		
92	(79) To facilitate simplification of compliance for entities, the ECCF should provide for the possibility to certify their cyber posture. Entities, notably those providing multiple types of services across several Member States, may face different cybersecurity and data security-related obligations under horizontal instruments, such as Regulation (EU) 2016/679 of the European Parliament and of the Council[1] and Directive (EU) 2022/2555 of the European Parliament and of the Council[2], as well as sector-specific instruments. In order to streamline the implementation of the overall cybersecurity regulatory framework and facilitate compliance therewith, it should be possible for Union legislation to provide for the possibility of entities to demonstrate their compliance with cybersecurity risk-	(79) To facilitate simplification of compliance for entities, the ECCF should provide for the possibility to certify their cyber posture. Entities, notably those providing multiple types of services across several Member States, may face different cybersecurity and data security-related obligations under horizontal instruments, such as Regulation (EU) 2016/679 of the European Parliament and of the Council[1] and Directive (EU) 2022/2555 of the European Parliament and of the Council[2], as well as sector-specific instruments. In order to streamline the implementation of the overall cybersecurity regulatory framework and facilitate compliance therewith, it should be possible for Union legislation to provide for the possibility of entities to demonstrate their compliance with cybersecurity risk-

	CLEAN Commission Proposal	VS.EC Council Mandate
	management requirements through a European cybersecurity certification certificate. A relevant scheme could contribute to streamlining compliance requirements arising from different regulatory instruments, without prejudice to their specific certification requirements. Such simplification measures have the potential to reduce administrative burden, unlocking resources to strengthen the operational cybersecurity preparedness of entities in critical sectors of the Union. _____ 1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj). 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 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, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).	management requirements through a European cybersecurity certification certificate. A relevant scheme could contribute to streamlining compliance requirements arising from different regulatory instruments, without prejudice to their specific certification requirements. Such simplification measures have the potential to reduce administrative burden, unlocking resources to strengthen the operational cybersecurity preparedness of entities in critical sectors of the Union. _____ 1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj). 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 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, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).
Recital 80		
93	(80) European certification of cybersecurity risk-management requirements developed within the ECCF should enable entities to demonstrate compliance with relevant Union legislation where a scheme covers the respective legal requirements laid down in such an act and where it provides so. On that basis, a Union legal act may also provide for a presumption of conformity with those requirements. Such schemes could contribute to improving the coherent implementation of cybersecurity requirements of Union legislation to level the playing field across Member States and ease the compliance burden.	(80) European certification of cybersecurity risk-management requirements developed within the ECCF should enable entities to demonstrate compliance with relevant Union legislation where a scheme covers the respective legal requirements laid down in such an act and where it provides so. On that basis, a Union legal act may also provide for a presumption of conformity with those requirements. Such schemes could contribute to improving the coherent implementation of cybersecurity requirements of Union legislation to level the playing field across Member States and ease the compliance burden.
Recital 81		
94	(81) The European cybersecurity certification framework should provide for the possibility to certify ICT processes, defined as a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service. A protection profile is an example of an ICT process, as specified under Commission Implementing Regulation (EU) 2024/482[1]. Another example of an ICT process	(81) The European cybersecurity certification framework should provide for the possibility to certify ICT processes, defined as a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service. A protection profile is an example of an ICT process, as specified under Commission Implementing Regulation (EU) 2024/482[1]. Another example of an ICT process

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	is the set of activities undertaken by a manufacturer to securely design and develop an ICT product, including the physical, logical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the design and implementation of an ICT product in its development environment. The certification of such activities is often referred to as 'site certification' in the context of a certification process under Commission Implementing Regulation (EU) 2024/482. _____ 1. Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) (OJ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).	is the set of activities undertaken by a manufacturer to securely design and develop an ICT product, including the physical, logical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the design and implementation of an ICT product in its development environment. The certification of such activities is often referred to as 'site certification' in the context of a certification process under Commission Implementing Regulation (EU) 2024/482. _____ 1. Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) (OJ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).
Recital 82		
95	(82) The definition of managed security services in this Regulation should be consistent with that of managed security service providers in Directive (EU) 2022/2555. Those services consist of carrying out, or providing assistance for, activities relating to their customers' cybersecurity risk management, and have gained increasing importance in the prevention and mitigation of incidents. Accordingly, the providers of those services are considered to be essential or important entities belonging to a sector of high criticality pursuant to Directive (EU) 2022/2555. 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. However, managed security service providers have themselves also been the target of cyberattacks and pose a particular risk because of their close integration in the operations of their customers. It is therefore necessary that essential and important entities within the meaning of Directive (EU) 2022/2555 exercise increased diligence in selecting managed security service providers.	(82) The definition of managed security services in this Regulation should be consistent with that of managed security service providers in Directive (EU) 2022/2555. Those services consist of carrying out, or providing assistance for, activities relating to their customers' cybersecurity risk management, and have gained increasing importance in the prevention and mitigation of incidents. Accordingly, the providers of those services are considered to be essential or important entities belonging to a sector of high criticality pursuant to Directive (EU) 2022/2555. 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. However, managed security service providers have themselves also been the target of cyberattacks and pose a particular risk because of their close integration in the operations of their customers. It is therefore necessary that essential and important entities within the meaning of Directive (EU) 2022/2555 exercise increased diligence in selecting managed security service providers.
Recital 83		

	CLEAN Commission Proposal	VS.EC Council Mandate
96	(83) European cybersecurity certification schemes are relevant to a wide community of stakeholders, such as providers of ICT solutions, conformity assessment bodies and users. To promote wide stakeholder engagement, the European Cybersecurity Certification Assembly ("the Assembly") should be organised at least once a year with the aim to foster collaboration between the Commission, ENISA, Member States and relevant stakeholders. It will play a pivotal role in identifying and addressing new cybersecurity challenges and strategic priorities for certification, and ensuring that certification schemes facilitate the secure integration of digital technologies and are fit for users' needs. The Assembly should foster Union leadership in certification activities and uphold the certification framework's ability to deliver trust for businesses, public authorities, and the public.	(83) European cybersecurity certification schemes are relevant to a wide community of stakeholders, such as providers of ICT solutions, conformity assessment bodies and users. To promote wide stakeholder engagement, the European Cybersecurity Certification Assembly ("the Assembly") should be organised at least once a year with the aim to foster collaboration between the Commission, ENISA, Member States and relevant stakeholders. It will play a pivotal role in identifying and addressing new cybersecurity challenges and strategic priorities for certification, and ensuring that certification schemes facilitate the secure integration of digital technologies and are fit for users' needs. The Assembly should foster Union leadership in certification activities and uphold the certification framework's ability to deliver trust for businesses, public authorities, and the public.
Recital 84		
97	(84) The Commission should maintain a dedicated website to ensure transparency by publishing up to date information on the implementation progress of the ECCF. The website should include information related to certification schemes under preparation, strategic priorities for upcoming certification schemes, requests to ENISA to prepare candidate certification schemes and information on adoption of certification schemes. The Commission website will complement ENISA's website on European cybersecurity certification schemes, which should offer comprehensive details on the technical preparation of candidate schemes and of the maintenance of schemes, focusing on issued European cybersecurity certificates and EU statements of conformity.	(84) The Commission should maintain a dedicated website to ensure transparency by publishing up to date information on the implementation progress of the ECCF. The website should include ***up-to-date*** information related to certification schemes under preparation***, including their development plan***, strategic priorities for upcoming certification schemes, requests to ENISA to prepare candidate certification schemes ~~*and*~~***,*** information on adoption of certification schemes ***and information on the Assembly meetings***. The Commission website will complement ENISA's website on European cybersecurity certification schemes, which should offer comprehensive details on the technical preparation of candidate schemes and of the maintenance of schemes, focusing on issued European cybersecurity certificates and EU statements of conformity.
Recital 85		
98	(85) In order to enhance the dialogue between the Union institutions and to contribute to a formal, open, transparent and inclusive consultation process, the Commission should take into account elements arising from the views expressed	(85) In order to enhance the dialogue between the Union institutions and to contribute to a formal, open, transparent and inclusive consultation process, the Commission should take into account elements arising from the views expressed

	CLEAN Commission Proposal	VS.EC Council Mandate
	by the European Parliament and by the Council and the European Cybersecurity Certification Assembly when evaluating this Regulation.	by the European Parliament and by the Council and the European Cybersecurity Certification Assembly when evaluating this Regulation.
Recital 86		
99	(86) Feasibility studies conducted by ENISA should help to prepare for the planning and development of cybersecurity certification schemes. The studies should incorporate the perspectives of relevant stakeholders and align the future certification schemes with ongoing research, development, and technological assessment activities, recognising, in particular, the contributions of Union and Member State research initiatives. Such studies can help to identify available standards and technical specifications. They should be carried out upon request from the Commission, or in accordance with the Union strategic priorities to ensure that the evolving technological landscape and cybersecurity needs are adequately addressed and reflected when requesting and developing schemes.	(86) *The requests of the Commission addressed to ENISA for preparation of candidate European cybersecurity certification schemes should set out appropriate development plans. In situations where additional time would be needed for the development of a given candidate scheme due to unforeseen circumstances, the Commission should adjust the request and related development plan accordingly.* Feasibility studies conducted by ENISA should help to prepare for the planning and development of cybersecurity certification schemes. The studies should incorporate the perspectives of relevant stakeholders and align the future certification schemes with ongoing research, development, and technological assessment activities, recognising, in particular, the contributions of Union and Member State research initiatives. Such studies can help to identify available standards and technical specifications. They should be carried out upon request from the Commission, or in accordance with the Union strategic priorities to ensure that the evolving technological landscape and cybersecurity needs are adequately addressed and reflected when requesting and developing schemes.
Recital 86a		
99a		*(86a) The main tasks of the ECCG should be to advise and assist the Commission in its work towards ensuring the consistent implementation and application of the European cybersecurity certification framework, to assist and closely cooperate with ENISA in the preparation of candidate cybersecurity certification schemes, to adopt opinions addressed to ENISA and the Commission. The opinions on candidate schemes may also be adopted jointly between the ECCG members. The ECCG should facilitate the exchange of good practices and expertise between the various national cybersecurity certification authorities that are responsible for the authorisation of conformity*

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
		assessment bodies and the issuance of European cybersecurity certificates.
Recital 87		
100	(87) The design of the candidate scheme and its coverage of security objectives and elements should be commensurate to the subject matter and scope of the certification object. For example, a certification scheme of cloud services might therefore address security objectives which are relevant for ICT services and organisational security. As another example, a security objective related to not including known exploitable vulnerabilities will likely not be relevant to certification of ICT processes.	(87) The design of the candidate scheme *should be proportionate and cost-efficient to ensure wide accessibility of certification, including for small and medium-sized enterprises. Furthermore,* ~~and~~ its coverage of security objectives and elements should be commensurate to the subject matter and scope of the certification object. For example, a certification scheme of cloud services might therefore address security objectives which are relevant for ICT services and organisational security. As another example, a security objective related to not including known exploitable vulnerabilities will likely not be relevant to certification of ICT processes. *At the same time, the security objectives should be future-proof and reflect the latest technological development, new emerging threats, as well as adoption of Union legislation setting out the demonstration of compliance and the presumption of conformity through European cybersecurity certification.*
Recital 88		
101	(88) In order to ensure that European cybersecurity certification schemes are implemented in a harmonised manner across Member States, it is necessary to provide for rules on the maintenance of the schemes. Maintenance activities are also necessary to ensure that the schemes and their supporting documentation remain up-to-date, especially in a cybersecurity field where the threat landscape and technologies constantly evolve. Certification schemes should therefore be designed and maintained in a way that avoids the risk that they are quickly outdated. Maintenance activities should typically involve drafting and updating supporting documentation, including technical specifications and guidelines, as well as identifying standards or technical specifications that are relevant to the scheme. The analysis of the functioning of the scheme, its potential shortcomings and necessary improvement, should also be part of the maintenance activities. In addition, maintenance activities should include information sharing between	(88) In order to ensure that European cybersecurity certification schemes are implemented in a harmonised manner across Member States, it is necessary to provide for rules on the maintenance of the schemes. Maintenance activities are also necessary to ensure that the schemes and their supporting documentation remain up-to-date, especially in a cybersecurity field where the threat landscape and technologies constantly evolve. Certification schemes should therefore be designed and maintained in a way that avoids the risk that they are quickly outdated. Maintenance activities should typically involve drafting and updating supporting documentation, including technical specifications and guidelines, as well as identifying standards or technical specifications that are relevant to the scheme. The analysis of the functioning of the scheme, its potential shortcomings and necessary improvement, should also be part of the maintenance activities. In addition, maintenance activities should include information sharing between

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	Member States with regard to on the implementation of the schemes and contributions to peer review and peer assessment mechanisms.	Member States with regard to on the implementation of the schemes and contributions to peer review and peer assessment mechanisms.
Recital 89		
102	(89) Due to the technical nature of the maintenance activities, ENISA should manage such activities, in cooperation with the Commission and with the support of the European Cybersecurity Certification Group (ECCG) and its relevant sub-group on maintenance. The establishment of the ECCG sub-group on maintenance allows gathering technical contributions and insights from Member States with a view to harmonising approaches.	(89) Due to the technical nature of the maintenance activities, ENISA should manage such activities, in cooperation with the Commission and with the support of the European Cybersecurity Certification Group (ECCG) and its relevant sub-group on maintenance. The establishment of the ECCG sub-group on maintenance allows gathering technical contributions and insights from Member States with a view to harmonising approaches.
Recital 89a		
102a		*(89a) The maintenance of schemes should be a collaborative effort primarily involving ENISA, the Member States and the Commission, in particular through the relevant ECCG subgroups co-chaired by the Commission and ENISA. ENISA in cooperation with the ECCG should lead the technical maintenance activities, including by drafting supporting documentation, for instance technical specifications, managing the activity and providing the secretariat to the ECCG subgroups. The Commission should ensure consistency of the activities and outputs with European cybersecurity certification schemes, as well as with relevant Union legislation, in particular in case where schemes provide presumption of conformity with such legislation. Member States' contribution to maintenance activities includes technical inputs, and national insights on the practical implementation of the scheme.*
Recital 90		
103	(90) Maintenance activities should entail interactions with relevant stakeholder groups to ensure that schemes remain market-relevant and up to date, including by sharing and receiving technical contributions. Such stakeholder groups can be standardisation organisations, conformity assessment bodies, vendors, users, public authorities, or trade associations. The specificities of each scheme,	(90) Maintenance activities should entail interactions with relevant stakeholder groups to ensure that schemes remain market-relevant and up to date, including by sharing and receiving technical contributions. Such stakeholder groups can be standardisation organisations, conformity assessment bodies, vendors, users, public authorities, or trade associations. The specificities of each scheme,

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	including their corresponding technical forums and industries, imply that it should be possible for technical contributions to be gathered in different ways from one scheme to the other. For some schemes, ENISA should be able to rely on an ad hoc working group that gathers experts from the public administrations of the Member States, Union entities, and the private sector. Technical contributions could also come from ISACs or standardisation organisations. ENISA should analyse which format is most suitable for each scheme and include a maintenance strategy in each candidate scheme.	including their corresponding technical forums and industries, imply that it should be possible for technical contributions to be gathered in different ways from one scheme to the other. For some schemes, ENISA should be able to rely on an ad hoc working group that gathers experts from the public administrations of the Member States, Union entities, and the private sector. Technical contributions could also come from ISACs or standardisation organisations. ENISA should analyse which format is most suitable for each scheme and include a maintenance strategy in each candidate scheme.
Recital 90a		
103a		*(90a) European cybersecurity certification schemes should be designed in a market and policy-driven manner. ENISA should conduct an analysis of a European cybersecurity certification scheme at least once every four years to evaluate the impact and effectiveness of the scheme, which also entails the analysis of the uptake by the market. Based on the evaluation, the Commission, after consulting the ECCG and ENISA, can withdraw implementing acts providing for a European cybersecurity certification scheme that does not display the effectiveness and impact in terms of increasing the level of cybersecurity within the Union. The withdrawal of a scheme should have an appropriate transition period, with certificates that were already issued remaining valid until their expiry. This should, where relevant, include related demonstration of compliance and the presumption of conformity, unless the respective legal acts provide otherwise.*
Recital 91		
104	(91) European cybersecurity certification schemes should rely on standards or technical specifications, notably for the definition of security requirements and evaluation methodologies. ENISA should be given the possibility to draft technical specifications to support the preparation and maintenance of schemes, in particular where deliverables from standardisation organisations are missing or not suitable to fulfil the objectives of the scheme. As part of the drafting process,	(91) European cybersecurity certification schemes should rely on standards or technical specifications, notably for the definition of security requirements and evaluation methodologies. ENISA should be given the possibility to draft technical specifications to support the preparation and maintenance of schemes, in particular where deliverables from standardisation organisations are missing or not suitable to fulfil the objectives of the scheme. As part of the drafting process,

	CLEAN Commission Proposal	VS.EC Council Mandate
	ENISA should be supported by the ECCG and, where applicable, the ad hoc working group set up for the relevant scheme. ENISA should also seek contributions from stakeholder groups. Additionally, ENISA should consider market acceptance, as well as European and international standards. Taking into account the quality of the technical specifications and the objectives of the scheme, it should be possible for the Commission to reference technical specifications drafted by ENISA in a European cybersecurity certification scheme.	ENISA should be supported by the ECCG and, where applicable, the ad hoc working group set up for the relevant scheme. ENISA should also seek contributions from stakeholder groups. Additionally, ENISA should consider market acceptance, as well as European and international standards. Taking into account the quality of the technical specifications and the objectives of the scheme, it should be possible for the Commission to reference technical specifications drafted by ENISA in a European cybersecurity certification scheme.
Recital 92		
105	(92) Technical specifications developed by ENISA and referenced in a scheme should be made available on the ENISA website on European cybersecurity certification schemes so that all interested parties can access them. However, in some specific cases, publication on the website could pose a risk to the cybersecurity of certified ICT products, ICT services, ICT processes, managed security services or cyber posture of entities and by extension to public safety. For example, technical specifications could contain precise information on new attack paths whose public availability would make it possible for malicious actors to use them. This type of information should be distributed in a restricted manner on a need-to-know basis to relevant stakeholders, such as national cybersecurity certification authorities, conformity assessment bodies and vendors being certified. Due to their restricted distribution, such technical specifications should not be referenced in European cybersecurity certification schemes and, therefore, should be of non-binding nature.	(92) Technical specifications developed by ENISA and referenced in a scheme should be made available on the ENISA website on European cybersecurity certification schemes so that all interested parties can access them. However, in some specific cases, publication on the website could pose a risk to the cybersecurity of certified ICT products, ICT services, ICT processes, managed security services or cyber posture of entities and by extension to public safety. For example, technical specifications could contain precise information on new attack paths whose public availability would make it possible for malicious actors to use them. This type of information should be distributed in a restricted manner on a need-to-know basis to relevant stakeholders, such as national cybersecurity certification authorities, conformity assessment bodies and vendors being certified. Due to their restricted distribution, such technical specifications should not be referenced in European cybersecurity certification schemes and, therefore, should be of non-binding nature.
Recital 93		
106	(93) The cyber posture certification schemes should be designed in a modular way, with a view to allowing demonstration of compliance and the presumption of conformity with relevant cybersecurity requirements set out in other Union legislation, where that legislation provides for that possibility. The presumption of conformity with the requirements of these legal acts will therefore only take	(93) The cyber posture certification schemes should be designed in a modular way, with a view to allowing demonstration of compliance and the presumption of conformity with relevant cybersecurity requirements set out in other Union legislation, where that legislation provides for that possibility. The presumption of conformity with the requirements of these legal acts will therefore only take

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	effect as a possible avenue to demonstrate compliance if the respective legal acts enable such presumption of conformity. The details of such a scheme, namely purpose, objectives or elements will therefore likely differ from those of other schemes. In particular, schemes for the certification of cyber posture of entities should be developed to provide for assessment of continuous conformity of an entity with Union legislation. It is therefore not necessary that cyber posture certification schemes cover all elements of the European cybersecurity certification schemes, such as assurance levels, and this should be reflected in the rules for the schemes.	effect as a possible avenue to demonstrate compliance if the respective legal acts enable such presumption of conformity, ***without prejudice to supervisory activities of the competent authorities***. The details of such a scheme, namely purpose, objectives or elements will therefore likely differ from those of other schemes. In particular, schemes for the certification of cyber posture of entities should be developed to provide for assessment of continuous conformity of an entity with Union legislation. It is therefore not necessary that cyber posture certification schemes cover all elements of the European cybersecurity certification schemes, such as assurance levels, and this should be reflected in the rules for the schemes.
Recital 94		
107	(94) A framework for cyber posture certification in the ECCF, allows for developing a scheme that enables entities providing services across several Member States to demonstrate compliance with the cybersecurity risk-management obligations laid down in Directive 2022/2555 of the European Parliament and of the Council. On that basis, with the ability to demonstrate compliance, entities can benefit from more coherent and less burdensome supervisory approaches across the internal market. The development of such a certification scheme should be facilitated by the adoption of implementing acts under Directive (EU) 2022/2555. Through extension profiles, a cyber posture certification scheme may demonstrate compliance with requirements where a Member State adopted or maintained provisions ensuring a higher level of cybersecurity in line with Directive (EU) 2022/2555. On this basis, an entity providing services across several Member States can demonstrate compliance with all relevant extension profiles through a single European cybersecurity certificate.	(94) A framework for cyber posture certification in the ECCF, allows for developing a scheme that enables entities providing services, ***including managed security services,*** across several Member States to demonstrate compliance with the cybersecurity risk-management obligations laid down in Directive 2022/2555 of the European Parliament and of the Council. On that basis, with the ability to demonstrate compliance, entities can benefit from more coherent and less burdensome supervisory approaches across the internal market. The development of such a certification scheme should be facilitated by the adoption of implementing acts under Directive (EU) 2022/2555. Through extension profiles, a cyber posture certification scheme may demonstrate compliance with requirements where a Member State adopted or maintained provisions ensuring a higher level of cybersecurity in line with Directive (EU) 2022/2555. On this basis, an entity providing services across several Member States can demonstrate compliance with all relevant extension profiles through a single European cybersecurity certificate.
Recital 95		
108	(95) The security objectives and the security requirements set out in European cybersecurity certification schemes for what pertains to product security should	(95) The security objectives and the security requirements set out in European cybersecurity certification schemes for what pertains to product security should

	CLEAN Commission Proposal	VS.EC Council Mandate
	be consistent with the essential cybersecurity requirements set out in Annex I to Regulation (EU) 2024/2847. This coherence is necessary to ensure that manufacturers whose products fall within the scope of Regulation (EU) 2024/2847 do not face contradictory requirements when certifying their products under a European cybersecurity certification scheme. Furthermore, consistency of requirements facilitates the presumption of conformity by Article 27 of Regulation (EU) 2024/2847 whereby manufacturers of products with digital elements that have been certified under a European cybersecurity certification scheme can benefit under certain conditions from presumption of conformity with the essential cybersecurity requirements set out in Annex I to that Regulation.	be consistent with the essential cybersecurity requirements set out in Annex I to Regulation (EU) 2024/2847. This coherence is necessary to ensure that manufacturers whose products fall within the scope of Regulation (EU) 2024/2847 do not face contradictory requirements when certifying their products under a European cybersecurity certification scheme. Furthermore, consistency of requirements facilitates the presumption of conformity by Article 27 of Regulation (EU) 2024/2847 whereby manufacturers of products with digital elements that have been certified under a European cybersecurity certification scheme can benefit under certain conditions from presumption of conformity with the essential cybersecurity requirements set out in Annex I to that Regulation.
Recital 96		
109	(96) Within the European cybersecurity certification scheme, it should be possible to specify an extension profile, by setting out additional or specific requirements for use cases, including additional capabilities such as enhanced product features, specialised service offerings or assets, optimised processes, and advanced security measures. Since extension profiles do not correspond to a specific assurance level, they should describe their purpose in detail, including the security threats addressed. Extension profiles are intended in particular to demonstrate compliance with specific standards and regulatory requirements, including, where applicable, requirements as regards additional cybersecurity risk-management measures laid down by a Member State following the minimum harmonisation principle in line with Directive (EU) 2022/2555.	(96) Within the European cybersecurity certification scheme, it should be possible to specify an extension profile, by setting out additional or specific requirements for use cases, including additional capabilities such as enhanced product features, specialised service offerings or assets, optimised processes, and advanced security measures. Since extension profiles do not correspond to a specific assurance level, they should describe their purpose in detail, including the security threats addressed. Extension profiles are intended in particular to demonstrate compliance with specific standards and regulatory requirements, including, where applicable, requirements as regards additional cybersecurity risk-management measures laid down by a Member State following the minimum harmonisation principle in line with Directive (EU) 2022/2555.
Recital 97		
110	(97) Without prejudice to the general peer review system to be put in place across all national cybersecurity certification authorities within the ECCF, it should be possible to include in the European cybersecurity certification schemes a peer-assessment mechanism for the bodies that issue European cybersecurity certificates for ICT products, ICT services, ICT processes, managed security	(97) Without prejudice to the general peer review system to be put in place across all national cybersecurity certification authorities within the ECCF, it should be possible to include in the European cybersecurity certification schemes a peer-assessment mechanism for the bodies that issue European cybersecurity certificates for ICT products, ICT services, ICT processes, managed security

	CLEAN Commission Proposal	VS.EC Council Mandate
	services and cyber posture of entities, in particular for those bodies that issue certificates with an assurance level 'high' under such schemes. Such bodies should also include certification bodies of the national cybersecurity certification authorities issuing certificates at assurance level 'high'. The ECCG should support the implementation of such peer-assessment mechanisms. The peer assessments should assess in particular whether the bodies concerned carry out their tasks in a harmonised way and may include appeal mechanisms.	services and cyber posture of entities, in particular for those bodies that issue certificates with an assurance level 'high' under such schemes. Such bodies should also include certification bodies of the national cybersecurity certification authorities issuing certificates at assurance level 'high'. The ECCG should support the implementation of such peer-assessment mechanisms. The peer assessments should assess in particular whether the bodies concerned carry out their tasks in a harmonised way and may include appeal mechanisms.
Recital 98		
111	(98) Crises such as wars, natural disasters, and pandemics might negatively impact certification activities. In crisis scenarios of this nature, it might not be feasible, for example, to ensure site security due to infrastructure destruction, cyberattacks, personnel unavailability, and the inaccessibility of the site. A European cybersecurity certification scheme should therefore specify temporary rules on continuity of certification activities during such scenarios.	(98) Crises such as wars, natural disasters, and pandemics might negatively impact certification activities. In crisis scenarios of this nature, it might not be feasible, for example, to ensure site security due to infrastructure destruction, cyberattacks, personnel unavailability, and the inaccessibility of the site. A European cybersecurity certification scheme should therefore specify temporary rules on continuity of certification activities during such scenarios.
Recital 99		
112	(99) Translating technical candidate schemes into implementing acts requires complex technical and legal knowledge and can create significant administrative burden. Moreover, certain elements of European cybersecurity certification schemes, such as vulnerability management or the conditions under which such marks or labels may be used, are cross-sectoral and may benefit from harmonised reference provisions. To ensure the quality of adopted European cybersecurity certification schemes and reduce compliance burden for businesses, the Commission should be empowered to adopt model provisions covering certain elements of European cybersecurity certification schemes.	(99) Translating technical candidate schemes into implementing acts requires complex technical and legal knowledge and can create significant administrative burden. Moreover, certain elements of European cybersecurity certification schemes, such as vulnerability management or the conditions under which such marks or labels may be used, are cross-sectoral and may benefit from harmonised reference provisions. To ensure the quality of adopted European cybersecurity certification schemes and reduce compliance burden for businesses, the Commission should be empowered to adopt model provisions covering certain elements of European cybersecurity certification schemes.
Recital 100		
113	(100) In order to ensure the consistency of the European cybersecurity certification framework, it should be possible within a European cybersecurity certification scheme to specify assurance levels for European cybersecurity	(100) In order to ensure the consistency of the European cybersecurity certification framework, it should be possible within a European cybersecurity certification scheme to specify assurance levels for European cybersecurity

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	certificates and EU statements of conformity issued under that scheme. A European cybersecurity certificate should refer to one of the assurance levels: 'basic', 'substantial' or 'high', while the EU statement of conformity should only refer to the assurance level 'basic'. The assurance levels should provide the corresponding rigour and depth of the evaluation of the ICT product, ICT service, ICT process, managed security service or cyber posture of an entity and should be characterised by reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to mitigate or prevent incidents. Each assurance level should be consistent among the different sectorial domains where certification is applied.	certificates and EU statements of conformity issued under that scheme. A European cybersecurity certificate should refer to one of the assurance levels: 'basic', 'substantial' or 'high', while the EU statement of conformity should only refer to the assurance level 'basic'. The assurance levels should provide the corresponding rigour and depth of the evaluation of the ICT product, ICT service, ICT process, managed security service or cyber posture of an entity and should be characterised by reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to mitigate or prevent incidents. Each assurance level should be consistent among the different sectorial domains where certification is applied.
Recital 101		
114	(101) The choice of the appropriate certification and associated security requirements by the users of European cybersecurity certificates should be based on an analysis of the risks associated with the use of the ICT products, ICT services, ICT processes, managed security services or the context of the certification of entities. Accordingly, the assurance level should be commensurate with the level of risk associated with the intended use of the ICT product, ICT service, ICT process, managed security services, or the operational environment and nature of the entity the cyber posture of which is subject to certification.	(101) The choice of the appropriate certification and associated security requirements by the users of European cybersecurity certificates should be based on an analysis of the risks associated with the use of the ICT products, ICT services, ICT processes, managed security services or the context of the certification of entities. Accordingly, the assurance level should be commensurate with the level of risk associated with the intended use of the ICT product, ICT service, ICT process, managed security services, or the operational environment and nature of the entity the cyber posture of which is subject to certification.
Recital 102		
115	(102) For assurance level 'basic', the evaluation should be guided at least by the following assurance components: the evaluation should at least include a review of the technical documentation of the ICT product, ICT service, ICT process, managed security service or cyber posture of an entity by the conformity assessment body. Where the certification includes ICT processes, the process used to design, develop and maintain an ICT product, ICT service, managed security service or cyber posture of an entity should also be subject to the technical review. Where a European cybersecurity certification scheme provides	(102) For assurance level 'basic', the evaluation should be guided at least by the following assurance components: the evaluation should at least include a review of the technical documentation of the ICT product, ICT service, ICT process, managed security service or cyber posture of an entity by the conformity assessment body. Where the certification includes ICT processes, the process used to design, develop and maintain an ICT product, ICT service, managed security service or cyber posture of an entity should also be subject to the technical review. Where a European cybersecurity certification scheme provides

	CLEAN Commission Proposal	VS.EC Council Mandate
	for a conformity self-assessment, it should be sufficient that the manufacturer or provider of ICT products, ICT services, ICT processes or managed security services, or the entity whose cyber posture of which is subject to certification, has carried out a self-assessment of the compliance of the ICT product, ICT service, ICT process, managed security service or cyber posture of an entity with the certification scheme.	for a conformity self-assessment, it should be sufficient that the manufacturer or provider of ICT products, ICT services, ICT processes or managed security services, or the entity whose cyber posture of which is subject to certification, has carried out a self-assessment of the compliance of the ICT product, ICT service, ICT process, managed security service or cyber posture of an entity with the certification scheme.
Recital 103		
116	(103) For assurance level 'substantial', the evaluation, in addition to the requirements for assurance level 'basic', should be guided at least by the verification of the compliance of the security functionalities of the ICT product, ICT service, ICT process, managed security service or cyber posture of an entity with its technical documentation.	(103) For assurance level 'substantial', the evaluation, in addition to the requirements for assurance level 'basic', should be guided at least by the verification of the compliance of the security functionalities of the ICT product, ICT service, ICT process, managed security service or cyber posture of an entity with its technical documentation.
Recital 104		
117	(104) For assurance level 'high', the evaluation, in addition to the requirements for assurance level 'substantial', should be guided at least by an efficiency testing which assesses the resistance of the security functionalities against elaborate cyberattacks performed by persons who have significant skills and resources. Conformity assessment activities should be performed in the European Economic Area for assurance level 'high' or where a scheme is designed to demonstrate compliance and provide for presumption of conformity with other Union legislation. This requirement is justified by the fact that assessment activities taking place outside the European Economic Area give rise to additional threats to cybersecurity, in particular the intellectual property of the evaluated ICT products, ICT services, ICT processes, managed security services or entities. For instance, the source code of an ICT product could be scrutinised when crossing the border of a third country, which constitutes a risk to intellectual property. Additionally, testing laboratories established in third countries do not operate in an environment that is concerned by the cybersecurity measures mandated by EU legislation, such as Directive (EU)	(104) For assurance level 'high', the evaluation, in addition to the requirements for assurance level 'substantial', should be guided at least by an efficiency testing which assesses the resistance of the security functionalities against elaborate cyberattacks performed by persons who have significant skills and resources. Conformity assessment activities should be performed in the European Economic Area for assurance level 'high' or where a scheme is designed to demonstrate compliance and provide for presumption of conformity with other Union legislation. This requirement is justified by the fact that assessment activities taking place outside the European Economic Area give rise to additional threats to cybersecurity, in particular the intellectual property of the evaluated ICT products, ICT services, ICT processes, managed security services or entities. For instance, the source code of an ICT product could be scrutinised when crossing the border of a third country, which constitutes a risk to intellectual property. Additionally, testing laboratories established in third countries do not operate in an environment that is concerned by the cybersecurity measures mandated by EU legislation, such as Directive (EU)

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	2022/2555 or Regulation (EU) 2024/2847. For instance, a testing laboratory may rely on a third-party cloud service provider which do not abide to the cybersecurity requirements of Directive (EU) 2022/2555. Nevertheless, a certification scheme should be allowed to provide for derogation mechanisms for instance related to site certification or in other instances where conformity assessment activities cannot be reasonably performed in the European Economic Area.	2022/2555 or Regulation (EU) 2024/2847. For instance, a testing laboratory may rely on a third-party cloud service provider which do not abide to the cybersecurity requirements of Directive (EU) 2022/2555. Nevertheless, a certification scheme should be allowed to provide for derogation mechanisms for instance related to site certification or in other instances where conformity assessment activities cannot be reasonably performed in the European Economic Area.
Recital 105		
118	(105) In some cases, different approaches to meet security objectives of a given assurance level might be required to address specifics of an ICT product, ICT service, ICT process, managed security services or cyber posture of entities. To allow for a more granular approach, it should be possible in a European cybersecurity certification scheme to specify one or several evaluation levels corresponding to one of the assurance levels. This will enable development of schemes where multiple evaluation levels designed for a different purpose will correspond to the level of security associated with a specific assurance level.	(105) In some cases, different approaches to meet security objectives of a given assurance level might be required to address specifics of an ICT product, ICT service, ICT process, managed security services or cyber posture of entities. To allow for a more granular approach, it should be possible in a European cybersecurity certification scheme to specify one or several evaluation levels corresponding to one of the assurance levels. This will enable development of schemes where multiple evaluation levels designed for a different purpose will correspond to the level of security associated with a specific assurance level. *Cyber posture schemes should be designed in a risk-based manner and could, therefore, include different evaluation levels taking into account the size, resources and operational capacity of entities, in particular small and medium-sized enterprises.*
Recital 106		
119	(106) European cybersecurity certification schemes should be allowed to provide for a conformity assessment to be carried out under the sole responsibility of the manufacturer or provider of ICT products, ICT services, ICT processes or managed security services, or the entity the cyber posture of which is certified ('conformity self-assessment'). In such cases, it should be sufficient that the manufacturer, provider or entity the cyber posture of which is certified, carries out all of the checks itself to ensure that the ICT products, ICT services, ICT processes, managed security service or cyber posture of an entity conform with	(106) European cybersecurity certification schemes should be allowed to provide for a conformity assessment to be carried out under the sole responsibility of the manufacturer or provider of ICT products, ICT services, ICT processes or managed security services, or the entity the cyber posture of which is certified ('conformity self-assessment'). In such cases, it should be sufficient that the manufacturer, provider or entity the cyber posture of which is certified, carries out all of the checks itself to ensure that the ICT products, ICT services, ICT processes, managed security service or cyber posture of an entity conform with

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	the European cybersecurity certification scheme. Conformity self-assessment should be considered to be appropriate for ICT products, ICT services, ICT processes, managed security service or cyber posture of entity that are of low complexity, that present a low risk to the public and that have a simple design or simple production mechanisms.	the European cybersecurity certification scheme. Conformity self-assessment should be considered to be appropriate for ICT products, ICT services, ICT processes, managed security service or cyber posture of entity that are of low complexity, that present a low risk to the public and that have a simple design or simple production mechanisms.
Recital 107		
120	(107) Where a European cybersecurity certification scheme allows for both conformity self-assessments and certifications of ICT products, ICT services, ICT processes, managed security services or cyber posture of entities, in such a case, the certification scheme should provide for clear and understandable means for consumers or other users to differentiate between self-assessed and third-party certified ICT products, ICT services, ICT processes, managed security services or cyber posture of entities.	(107) Where a European cybersecurity certification scheme allows for both conformity self-assessments and certifications of ICT products, ICT services, ICT processes, managed security services or cyber posture of entities, in such a case, the certification scheme should provide for clear and understandable means for consumers or other users to differentiate between self-assessed and third-party certified ICT products, ICT services, ICT processes, managed security services or cyber posture of entities.
Recital 108		
121	(108) The manufacturer or provider of ICT products, ICT services, ICT processes or managed security services, or the entities the cyber posture of which is certified, should be able to issue and sign the EU statement of conformity as part of the conformity assessment procedure. An EU statement of conformity is a document that states that a specific ICT product, ICT service, ICT process, managed security service or the cyber posture of an entity complies with the requirements of the European cybersecurity certification scheme. By issuing and signing the EU statement of conformity, the manufacturer or provider of ICT products, ICT services, ICT processes or managed security services, or the entity the cyber posture of which is certified, assumes responsibility for the compliance of the ICT product, ICT service, ICT process, managed security service or the cyber posture of the entity with the security requirements of the European cybersecurity certification scheme. A copy of the EU statement of conformity should be submitted to the national cybersecurity certification authority and to ENISA.	(108) The manufacturer or provider of ICT products, ICT services, ICT processes or managed security services, or the entities the cyber posture of which is certified, should be able to issue and sign the EU statement of conformity as part of the conformity assessment procedure. An EU statement of conformity is a document that states that a specific ICT product, ICT service, ICT process, managed security service or the cyber posture of an entity complies with the requirements of the European cybersecurity certification scheme. By issuing and signing the EU statement of conformity, the manufacturer or provider of ICT products, ICT services, ICT processes or managed security services, or the entity the cyber posture of which is certified, assumes responsibility for the compliance of the ICT product, ICT service, ICT process, managed security service or the cyber posture of the entity with the security requirements of the European cybersecurity certification scheme. A copy of the EU statement of conformity should be submitted to the national cybersecurity certification authority and to ENISA.

PUBLIC

	CLEAN	Commission Proposal	VS.EC	Council Mandate
Recital 109				
122		(109) Manufacturers or providers of ICT products, ICT services, ICT processes or managed security services, or entities the cyber posture of which is certified, should make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity with a European cybersecurity certification scheme available to the competent national cybersecurity certification authority for a period provided for in the relevant European cybersecurity certification scheme and in line with applicable Union legislation. The technical documentation should specify the requirements applicable under the scheme to the extent relevant to the conformity self-assessment. The technical documentation should be so compiled as to enable the assessment of whether an ICT product, ICT service, ICT process or managed security service, or cyber posture of the entity complies with the requirements applicable under the scheme.		(109) Manufacturers or providers of ICT products, ICT services, ICT processes or managed security services, or entities the cyber posture of which is certified, should make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity with a European cybersecurity certification scheme available to the competent national cybersecurity certification authority for a period provided for in the relevant European cybersecurity certification scheme and in line with applicable Union legislation. The technical documentation should specify the requirements applicable under the scheme to the extent relevant to the conformity self-assessment. The technical documentation should be so compiled as to enable the assessment of whether an ICT product, ICT service, ICT process or managed security service, or cyber posture of the entity complies with the requirements applicable under the scheme.
Recital 110				
123		(110) European cybersecurity certificates and EU statements of conformity should help users make informed choices. Therefore, relevant information should be published on a website maintained by ENISA. Furthermore, ICT products, ICT services, and ICT processes that have been certified or for which an EU statement of conformity has been issued should be accompanied by structured information that is adapted to the expected technical level of the intended user. All users should have access to information regarding the reference number of the certification scheme, the issuing authority or body, and, where applicable, the assurance level, or should be able to obtain a copy of the European cybersecurity certificate. That information should be regularly updated and made available on a dedicated website on European cybersecurity certification schemes. Furthermore, in order to ensure continuous accessibility, manufacturers and providers should be required to notify the relevant certification body if the location of the online or, where relevant, physical information changes.		(110) European cybersecurity certificates and EU statements of conformity should help users make informed choices. Therefore, relevant information should be published on a website maintained by ENISA. Furthermore, ICT products, ICT services, and ICT processes that have been certified or for which an EU statement of conformity has been issued should be accompanied by structured information that is adapted to the expected technical level of the intended user. All users should have access to information regarding the reference number of the certification scheme, the issuing authority or body, and, where applicable, the assurance level, or should be able to obtain a copy of the European cybersecurity certificate. That information should be regularly updated and made available on a dedicated website on European cybersecurity certification schemes. Furthermore, in order to ensure continuous accessibility, manufacturers and providers should be required to notify the relevant certification body if the location of the online or, where relevant, physical information changes.

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Recital 111		
124	(111) A conformity assessment is a procedure for evaluating whether specified requirements relating to an ICT product, ICT service, ICT process, managed security service or entity have been fulfilled. That procedure is carried out by an independent third party that is not the manufacturer or provider of the ICT products, ICT services, ICT processes or managed security services that are being certified, nor the entity the cyber posture of which is being assessed. A European cybersecurity certificate should be issued following the successful evaluation of an ICT product, ICT service, ICT process, managed security service or cyber posture of the entity. A European cybersecurity certificate should be considered to be a confirmation that the evaluation has been properly carried out.	(111) A conformity assessment is a procedure for evaluating whether specified requirements relating to an ICT product, ICT service, ICT process, managed security service or entity have been fulfilled. That procedure is carried out by an independent third party that is not the manufacturer or provider of the ICT products, ICT services, ICT processes or managed security services that are being certified, nor the entity the cyber posture of which is being assessed. A European cybersecurity certificate should be issued following the successful evaluation of an ICT product, ICT service, ICT process, managed security service or cyber posture of the entity. A European cybersecurity certificate should be considered to be a confirmation that the evaluation has been properly carried out.
Recital 112		
125	(112) The strict separation of the supervisory and certification activities is important to avoid distortions and interferences that may be caused in situations where the entity supervising the market is also competing in the same market. Consequently, activities where the national cybersecurity certification authorities merely carry out their supervisory role, such as by providing prior approval to the issuance of a certificate, should not require further internal separation from other supervisory activities. This includes, for example, a situation where the national cybersecurity certification authority actively gathers information throughout the certification process carried out by private conformity assessment bodies and then gives its opinion on the issuance of the certificate by those bodies ('prior approval model').	(112) The strict separation of the supervisory and certification activities is important to avoid distortions and interferences that may be caused in situations where the entity supervising the market is also competing in the same market. Consequently, activities where the national cybersecurity certification authorities merely carry out their supervisory role, such as by providing prior approval to the issuance of a certificate, should not require further internal separation from other supervisory activities. This includes, for example, a situation where the national cybersecurity certification authority actively gathers information throughout the certification process carried out by private conformity assessment bodies and then gives its opinion on the issuance of the certificate by those bodies ('prior approval model').
Recital 113		
126	(113) European cybersecurity certification schemes should specify the conditions under which ICT products, ICT services, ICT processes, managed security services or cyber posture of an entity may need to be recertified or under which the scope of a specific European cybersecurity certificate may need to be	(113) European cybersecurity certification schemes should specify the conditions under which ICT products, ICT services, ICT processes, managed security services or cyber posture of an entity may need to be recertified or under which the scope of a specific European cybersecurity certificate may need to be

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	reduced. Furthermore, European cybersecurity certification schemes should take into account any possible adverse effects of any subsequently detected vulnerabilities or nonconformities concerning the certified ICT product, ICT service, ICT process, managed security service or cyber posture of an entity with regard to conformity with the security requirements of that certificate.	reduced. Furthermore, European cybersecurity certification schemes should take into account any possible adverse effects of any subsequently detected vulnerabilities or nonconformities concerning the certified ICT product, ICT service, ICT process, managed security service or cyber posture of an entity with regard to conformity with the security requirements of that certificate.
Recital 114		
127	(114) Harmonisation plays a crucial role in ensuring robust cybersecurity and enhancing market access for businesses. In contrast, fragmentation and the lack of mutual recognition of certificates pose significant barriers to the seamless flow of data, thereby increasing operational costs for Union industry. To mitigate those challenges, it is essential to avoid fragmentation both in the scope of the security controls and in the conformity assessment methods throughout the Union.	(114) Harmonisation plays a crucial role in ensuring robust cybersecurity and enhancing market access for businesses. In contrast, fragmentation and the lack of mutual recognition of certificates pose significant barriers to the seamless flow of data, thereby increasing operational costs for Union industry. To mitigate those challenges, it is essential to avoid fragmentation both in the scope of the security controls and in the conformity assessment methods throughout the Union.
Recital 115		
128	(115) Member States should inform the Commission and the ECCG sufficiently in advance before adopting new national cybersecurity certification schemes for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities in order to help the Commission and the ECCG evaluate the impact of the new national cybersecurity certification scheme on the proper functioning of the internal market, and in light of any strategic interest in requesting a European cybersecurity certification scheme.	(115) Member States should inform the Commission and the ECCG sufficiently in advance before adopting new national cybersecurity certification schemes for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities in order to help the Commission and the ECCG evaluate the impact of the new national cybersecurity certification scheme on the proper functioning of the internal market, and in light of any strategic interest in requesting a European cybersecurity certification scheme. *The Commission could also suggest the withdrawal of a national cybersecurity certification scheme in line with the development plan of a European cybersecurity certification scheme that has already been requested and covers the same scope. Such withdrawal before the adoption of a European cybersecurity certification scheme should be at the discretion of Member States.*
Recital 116		
129	(116) References in national legislation to national standards which have ceased to be effective due to the entry into force of a European cybersecurity	(116) References in national legislation to national standards which have ceased to be effective due to the entry into force of a European cybersecurity

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	certification scheme can be a source of confusion. Therefore, where relevant, Member States should reflect the adoption of a European cybersecurity certification scheme in their national legislation.	certification scheme can be a source of confusion. Therefore, where relevant, Member States should reflect the adoption of a European cybersecurity certification scheme in their national legislation.
Recital 117		
130	(117) With a view to facilitating the growth of a reliable internal market, while also creating partnerships with third countries, the certification process established within the ECCF should be implemented in a manner that facilitates international recognition, mutual recognition and alignment with international standards.	(117) With a view to facilitating the growth of a reliable internal market, while also creating partnerships with third countries, the certification process established within the ECCF should be implemented in a manner that facilitates international recognition, mutual recognition and alignment with international standards.
Recital 118		
131	(118) In order to further facilitate trade, and recognising that ICT supply chains are international, mutual recognition agreements concerning European cybersecurity certificates may be concluded by the Union in accordance with Article 218 TFEU. The Commission should be empowered to adopt implementing acts to unilaterally recognise the equivalence of third country certificates with European cybersecurity certificates. It should be possible to provide specific conditions for such recognition of third country certificates.	(118) In order to further facilitate trade, and recognising that ICT supply chains are international, mutual recognition agreements concerning European cybersecurity certificates may be concluded by the Union in accordance with Article 218 TFEU. The Commission should be empowered to adopt implementing acts to unilaterally recognise the equivalence of third country certificates with European cybersecurity certificates. It should be possible to provide specific conditions for such recognition of third country certificates.
Recital 119		
132	(119) In order to achieve equivalent implementation of the framework throughout the Union, to facilitate mutual recognition and to promote the overall acceptance of European cybersecurity certificates and EU statements of conformity, it is necessary to put in place a system of peer review between national cybersecurity certification authorities. Peer review should cover procedures for supervising the compliance of ICT products, ICT services, ICT processes, managed security services and cyber posture of entities with European cybersecurity certificates, for monitoring the obligations of manufacturers or providers of ICT products, ICT services, ICT processes, managed security services and certified entities who carry out the conformity self-assessment, for	(119) In order to achieve equivalent implementation of the framework throughout the Union, to facilitate mutual recognition and to promote the overall acceptance of European cybersecurity certificates and EU statements of conformity, it is necessary to put in place a system of peer review between national cybersecurity certification authorities. Peer review should cover procedures for supervising the compliance of ICT products, ICT services, ICT processes, managed security services and cyber posture of entities with European cybersecurity certificates, for monitoring the obligations of manufacturers or providers of ICT products, ICT services, ICT processes, managed security services and certified entities who carry out the conformity self-assessment, for

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	monitoring conformity assessment bodies, as well as the appropriateness of the expertise of the staff of bodies issuing certificates for assurance level 'high'. ENISA should participate in the peer reviews as observer and support the organisation of the peer review mechanism and peer reviews, including by developing relevant guidance documents and templates, in cooperation with the Commission and the ECCG. ENISA should also make publicly available on their website on European cybersecurity certification schemes the information on the schedule of peer reviews and the list of peer-reviewed national cybersecurity certification authorities that are to carry out the schedule. Commission Implementing Regulation (EU) 2025/2540[1], adopted under Regulation (EU) 2019/881 establishes the plan for peer reviews which is being utilised by the adopted European cybersecurity certification schemes. It is necessary to ensure the continuation of the peer reviews. Nevertheless, the Commission should be able, by means of implementing acts, where needed, to establish a new plan for peer reviews of at least five years, as well as to lay down criteria and methodologies for the operation of the peer review system. _____ 1. Commission Implementing Regulation (EU) 2025/2540 of 9 December 2025 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the establishment of the plan for peer review (OJ L 2540, 12.12.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/2540/oj).	monitoring conformity assessment bodies, as well as the appropriateness of the expertise of the staff of bodies issuing certificates for assurance level 'high'. ENISA should participate in the peer reviews as observer and support the organisation of the peer review mechanism and peer reviews, including by developing relevant guidance documents and templates, in cooperation with the Commission and the ECCG. ENISA should also make publicly available on their website on European cybersecurity certification schemes the information on the schedule of peer reviews and the list of peer-reviewed national cybersecurity certification authorities that are to carry out the schedule. Commission Implementing Regulation (EU) 2025/2540[1], adopted under Regulation (EU) 2019/881 establishes the plan for peer reviews which is being utilised by the adopted European cybersecurity certification schemes. It is necessary to ensure the continuation of the peer reviews. Nevertheless, the Commission should be able, by means of implementing acts, where needed, to establish a new plan for peer reviews of at least five years, as well as to lay down criteria and methodologies for the operation of the peer review system. _____ 1. Commission Implementing Regulation (EU) 2025/2540 of 9 December 2025 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the establishment of the plan for peer review (OJ L 2540, 12.12.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/2540/oj).
Recital 120		
133	(120) Once a European cybersecurity certification scheme is adopted, manufacturers or providers of ICT products, ICT services, ICT processes, managed security services or the entities the cyber posture of which is the subject of certification, should be able to submit applications for certification of their ICT products, ICT services, ICT processes, managed security services or cyber posture to the conformity assessment body of their choice anywhere in the Union. Conformity assessment bodies should be accredited by a national accreditation body if they comply with the requirements set out in this	(120) Once a European cybersecurity certification scheme is adopted, manufacturers or providers of ICT products, ICT services, ICT processes, managed security services or the entities the cyber posture of which is the subject of certification, should be able to submit applications for certification of their ICT products, ICT services, ICT processes, managed security services or cyber posture to the conformity assessment body of their choice anywhere in the Union. Conformity assessment bodies should be accredited by a national accreditation body if they comply with the requirements set out in this

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	Regulation, and, where applicable, with the requirements specified by the Commission in accordance with this Regulation. The system set out in this Regulation should be complemented by the accreditation system provided for in Regulation (EC) No 765/2008 of the European Parliament and of the Council[1]. _____ 1. Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).	Regulation, and, where applicable, with the requirements specified by the Commission in accordance with this Regulation. The system set out in this Regulation should be complemented by the accreditation system provided for in Regulation (EC) No 765/2008 of the European Parliament and of the Council[1]. _____ 1. Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).
Recital 121		
134	(121) Conformity assessment bodies that have been accredited or notified under existing Union legislation, in particular Regulation (EU) 2024/2847 or Implementing Regulation (EU) 2024/482, might possess competencies that are relevant to newly adopted European cybersecurity certification schemes. To avoid unnecessary financial and administrative burden, it is appropriate to create synergies for the accreditation of conformity assessment bodies under this Regulation. For this reason, the accreditation requirements of the schemes should be established in such a way that there is as much alignment as possible with requirements relating to notified bodies set out in Regulation (EU) 2024/2847 and accreditation requirements under Implementing Regulation (EU) 2024/482. In addition, conformity assessment bodies that undergo an accreditation process under this Regulation should be able to rely on previous results of evaluation of their competences under other Union legislation, whenever there is an overlap in the accreditation requirements.	(121) Conformity assessment bodies that have been accredited or notified under existing Union legislation, in particular Regulation (EU) 2024/2847 or Implementing Regulation (EU) 2024/482, might possess competencies that are relevant to newly adopted European cybersecurity certification schemes. To avoid unnecessary financial and administrative burden, it is appropriate to create synergies for the accreditation of conformity assessment bodies under this Regulation. For this reason, the accreditation requirements of the schemes should be established in such a way that there is as much alignment as possible with requirements relating to notified bodies set out in Regulation (EU) 2024/2847 and accreditation requirements under Implementing Regulation (EU) 2024/482. In addition, conformity assessment bodies that undergo an accreditation process under this Regulation should be able to rely on previous results of evaluation of their competences under other Union legislation, whenever there is an overlap in the accreditation requirements.
Recital 122		
135	(122) With a view to facilitating harmonised conformity assessment services across the Union, it should be possible to set out in a European cybersecurity certification scheme additional or specific requirements for conformity assessment bodies. In the context of certification, an authorisation should be	(122) With a view to facilitating harmonised conformity assessment services across the Union, it should be possible to set out in a European cybersecurity certification scheme additional or specific requirements for conformity assessment bodies. In the context of certification, an authorisation should be

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	understood as a decision by a national cybersecurity certification authority that a conformity assessment body meets the specific or additional requirements set out in a European cybersecurity certification scheme, to carry out a specific conformity assessment activity.	understood as a decision by a national cybersecurity certification authority that a conformity assessment body meets the specific or additional requirements set out in a European cybersecurity certification scheme, to carry out a specific conformity assessment activity.
Recital 123		
136	(123) Where a European cybersecurity certification scheme sets out additional or specific requirements in accordance with this Regulation, the conformity assessment bodies should be authorised by the national cybersecurity certification authorities to carry out tasks under such scheme. In order to avoid multiple authorisation, to enhance acceptance and recognition of authorisation decisions and to carry out effective monitoring of authorised conformity assessment bodies, conformity assessment bodies should request authorisation by the national cybersecurity certification authority of the Member State in which they are established. Nevertheless, it is necessary to ensure that a conformity assessment body is able to request authorisation in another Member State in the event that there is no national cybersecurity certification authority in its own Member State or where the national cybersecurity certification authority does not have the competence to provide the authorisation services requested. In such cases, appropriate cooperation and exchange of information between national cybersecurity certification authorities should be ensured. The Commission should be empowered to adopt implementing acts establishing the procedures for authorisation, including for cross-border cooperation with regard to authorisation.	(123) Where a European cybersecurity certification scheme sets out additional or specific requirements in accordance with this Regulation, the conformity assessment bodies should be authorised by the national cybersecurity certification authorities to carry out tasks under such scheme. In order to avoid multiple authorisation, to enhance acceptance and recognition of authorisation decisions and to carry out effective monitoring of authorised conformity assessment bodies, conformity assessment bodies should request authorisation by the national cybersecurity certification authority of the Member State in which they are established. Nevertheless, it is necessary to ensure that a conformity assessment body is able to request authorisation in another Member State in the event that there is no national cybersecurity certification authority in its own Member State or where the national cybersecurity certification authority does not have the competence to provide the authorisation services requested. In such cases, appropriate cooperation and exchange of information between national cybersecurity certification authorities should be ensured. The Commission should be empowered to adopt implementing acts establishing the procedures for authorisation, including for cross-border cooperation with regard to authorisation.
Recital 124		
137	(124) In order to safeguard the level of protection required for an ICT product, ICT service, ICT process, managed security service or cyber posture of an entity, it is essential that conformity assessment subcontractors and subsidiaries are required to meet the same requirements as the notified conformity assessment bodies in relation to the performance of conformity assessment tasks. Accordingly, a conformity assessment body should have the appropriate	(124) In order to safeguard the level of protection required for an ICT product, ICT service, ICT process, managed security service or cyber posture of an entity, it is essential that conformity assessment subcontractors and subsidiaries are required to meet the same requirements as the notified conformity assessment bodies in relation to the performance of conformity assessment tasks. Accordingly, a conformity assessment body should have the appropriate

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	competence and be able to verify that the applicable requirements are met by its subcontractors.	competence and be able to verify that the applicable requirements are met by its subcontractors.
Recital 125		
138	(125) The extent to which the conformity assessment body intends to rely on subcontractors established outside the Union, or have access to personnel or facilities outside the Member State of notification should be appropriately assessed by the notifying authority. The public authority of a Member State should have the possibility to decide that it cannot take the overall responsibility as a national cybersecurity certification authority for such an arrangement, and to withdraw or limit the scope of the notification.	(125) The extent to which the conformity assessment body intends to rely on subcontractors established outside the Union, or have access to personnel or facilities outside the Member State of notification should be appropriately assessed by the notifying authority. The public authority of a Member State should have the possibility to decide that it cannot take the overall responsibility as a national cybersecurity certification authority for such an arrangement, and to withdraw or limit the scope of the notification.
Recital 126		
139	(126) In order to evaluate the cybersecurity requirements for ICT products, ICT services, ICT processes, managed security services or the cyber posture of entities, accredited conformity assessment bodies should be notified by the national cybersecurity certification authorities to the Commission and the other Member States. Notification of accredited and, where applicable, authorised conformity assessment bodies indicates that those bodies can be trusted in performing evaluation and certification activities in accordance with this Regulation and the European cybersecurity certification scheme, contributing to the overall reputation of European cybersecurity certification. It is therefore essential to ensure that conformity assessment bodies that have been notified meet their requirements and fulfil their obligations over time, and that the list of notified conformity assessment bodies is kept up to date.	(126) In order to evaluate the cybersecurity requirements for ICT products, ICT services, ICT processes, managed security services or the cyber posture of entities, accredited conformity assessment bodies should be notified by the national cybersecurity certification authorities to the Commission and the other Member States. Notification of accredited and, where applicable, authorised conformity assessment bodies indicates that those bodies can be trusted in performing evaluation and certification activities in accordance with this Regulation and the European cybersecurity certification scheme, contributing to the overall reputation of European cybersecurity certification. It is therefore essential to ensure that conformity assessment bodies that have been notified meet their requirements and fulfil their obligations over time, and that the list of notified conformity assessment bodies is kept up to date.
Recital 127		
140	(127) Commission Implementing Regulation (EU) 2024/3143[1] adopted under Regulation (EU) 2019/881 establishes the circumstances, formats and procedures for notifications of conformity assessment bodies which are being utilised by the adopted European cybersecurity certification schemes. It is	(127) Commission Implementing Regulation (EU) 2024/3143[1] adopted under Regulation (EU) 2019/881 establishes the circumstances, formats and procedures for notifications of conformity assessment bodies which are being utilised by the adopted European cybersecurity certification schemes. It is

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	therefore necessary to ensure the continuation of the notification activities. Nevertheless, the Commission should be empowered to adopt implementing acts to adjust those circumstances, procedures and formats for the notification of conformity assessment bodies. In this context, the Commission should draw on the experience gained in the context of existing schemes, and seek alignment with other relevant Union legislation and frameworks, in particular Regulation (EU) 2024/2847 and the new legislative framework, in view of reducing compliance burden for conformity assessment bodies active under different legal instruments. _____ 1. Commission Implementing Regulation (EU) 2024/3143 of 18 December 2024 establishing the circumstances, formats and procedures for notifications pursuant to Article 61(5) of Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (OJ L 3143, 19.12.2025, ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).	therefore necessary to ensure the continuation of the notification activities. Nevertheless, the Commission should be empowered to adopt implementing acts to adjust those circumstances, procedures and formats for the notification of conformity assessment bodies. In this context, the Commission should draw on the experience gained in the context of existing schemes, and seek alignment with other relevant Union legislation and frameworks, in particular Regulation (EU) 2024/2847 and the new legislative framework, in view of reducing compliance burden for conformity assessment bodies active under different legal instruments. _____ 1. Commission Implementing Regulation (EU) 2024/3143 of 18 December 2024 establishing the circumstances, formats and procedures for notifications pursuant to Article 61(5) of Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (OJ L 3143, 19.12.2025, ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).
Recital 127a		
140a		*(127a) The Commission and the Member States should act when doubt arises about the competence of a notified conformity assessment body, either at the moment of notification or thereafter. Should the Commission consider, on its own initiative or after complaint, that a notified conformity assessment body does not comply with the requirements or fulfil its responsibilities, it should inform the national cybersecurity certification authority and ask for appropriate documented evidence concerning the basis for the notification of the competence of the body. Where a national cybersecurity certification authority has ascertained or has been informed that a notified conformity assessment body no longer meets the requirements laid down in this Regulation, or that it is failing to fulfil its obligations, the national cybersecurity certification authority should, depending on the seriousness of the failure, suspend or withdraw the notification after immediately contacting the body in question and inform the Commission and the other Member States accordingly. The body in question should have the*

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
		possibility to appeal against such a decision. The Commission can withdraw a notified body from the NANDO list on its own initiative only when the Court of Justice of the European Union declares a Member State to be in infringement of this Regulation and, consequently, declares a notification to be invalid.
Recital 128		
141	(128) Information and communication technology (ICT) supply chains are composed of a linked set of resources and processes between economic operators. ICT supply chains play a crucial role in sustaining societal stability and driving economic activity across the Union. They also play a critical role in enabling the digital infrastructure in the Union and underpin the functioning of Union society and economy. ICT supply chains enable the manufacture, production, distribution, and maintenance of ICT services, ICT systems and ICT products that underpin various critical and highly critical sectors, including healthcare, finance, transportation, telecommunication, energy and customs. The security of the ICT supply chains of those critical sectors may also have impact on the security of defence and military infrastructure, where this infrastructure relies on civilian critical sectors and their ICT supply chains. However, according to the report on the status of the cybersecurity threats issued by ENISA (ENISA Threat Landscape 2025)[1], attacks against supply chains are amongst the five prime threats to cybersecurity showing that attackers actively leveraging indirect pathways through third-party providers and dependencies. Disruption of ICT supply chains can impede the pursuit of economic activities in the internal market, generate financial loss, undermine user confidence and cause major damage to the Union's economy and society. Cybersecurity preparedness and effectiveness are therefore more essential than ever to the proper functioning of the internal market. _____ 1. ENISA Threat Landscape 2025, October 2025.	(128) Information and communication technology (ICT) supply chains are composed of a linked set of resources and processes between economic operators. ICT supply chains play a crucial role in sustaining societal stability and driving economic activity across the Union. They also play a critical role in enabling the digital infrastructure in the Union and underpin the functioning of Union society and economy. ICT supply chains enable the manufacture, production, distribution, and maintenance of ICT services, ICT systems and ICT products that underpin various critical and highly critical sectors, including healthcare, finance, transportation, telecommunication, energy and customs. The security of the ICT supply chains of those critical sectors may also have impact on the security of defence and military infrastructure, where this infrastructure relies on civilian critical sectors and their ICT supply chains. However, according to the report on the status of the cybersecurity threats issued by ENISA (ENISA Threat Landscape 2025)[1], attacks against supply chains are amongst the five prime threats to cybersecurity showing that attackers actively leveraging indirect pathways through third-party providers and dependencies. Disruption of ICT supply chains can impede the pursuit of economic activities in the internal market, generate financial loss, undermine user confidence and cause major damage to the Union's economy and society. Cybersecurity preparedness and effectiveness are therefore more essential than ever to the proper functioning of the internal market. _____ 1. ENISA Threat Landscape 2025, October 2025.
Recital 129		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
142	(129) Beyond technical risks which are addressed by Directive (EU) 2022/55 of the European Parliament and of the Council[1], Regulation (EU) 2024/2847 of the European Parliament and of the Council[2] and the European cybersecurity certification Framework established by Regulation (EU) 2019/881, ICT supply chains are increasingly exposed to risks of a non-technical nature. Such non-technical risks may be linked, but not limited, to the jurisdiction to which a supplier of certain components is subject, in particular where a third country or threat actors controlled from that country engage in economic espionage, carry out malicious cyber activities or campaigns against the Union or its Member States, or engages in irresponsible State behaviour in cyberspace. Non-technical risks can also be linked to concealed vulnerabilities or backdoors or potential systemic supply disruptions, in particular in the case of technological lock-in or supplier dependency. For instance, kill switches could be used to negatively impact the availability of communication networks and electricity grids. _____ 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 du 27.12.2022, p. 80-152, ELI: https://eur-lex.europa.eu/eli/dir/2022/2555/oj). 2. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024, ELI: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng).	(129) Beyond technical risks which are addressed by Directive (EU) 2022/55 of the European Parliament and of the Council[1], Regulation (EU) 2024/2847 of the European Parliament and of the Council[2] and the European cybersecurity certification Framework established by Regulation (EU) 2019/881, ICT supply chains are increasingly exposed to risks of a non-technical nature. Such non-technical risks may be linked, but not limited, to the jurisdiction to which a supplier of certain components is subject, in particular where a third country or threat actors controlled from that country engage in economic espionage, carry out malicious cyber activities or campaigns against the Union or its Member States, or engages in irresponsible State behaviour in cyberspace. Non-technical risks can also be linked to concealed vulnerabilities or backdoors or potential systemic supply disruptions, in particular in the case of technological lock-in or supplier dependency. For instance, kill switches could be used to negatively impact the availability of communication networks and electricity grids. _____ 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 du 27.12.2022, p. 80-152, ELI: https://eur-lex.europa.eu/eli/dir/2022/2555/oj). 2. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024, ELI: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng).
Recital 130		
143	(130) The Joint Communication on Strengthening EU economic security[1] underlined the risk of third countries gaining access to sensitive information and data in the Union or its Member States, either as a result of industrial espionage, their supply of hardware or software used in certain products or due to their ownership and control of certain businesses possessing sensitive information and	(130) The Joint Communication on Strengthening EU economic security[1] underlined the risk of third countries gaining access to sensitive information and data in the Union or its Member States, either as a result of industrial espionage, their supply of hardware or software used in certain products or due to their ownership and control of certain businesses possessing sensitive information and

	CLEAN Commission Proposal	VS.EC Council Mandate
	data. It also underlined the risk of the Union's critical infrastructure - including critical transport, space systems, energy and communications infrastructure, in particular those that are identified as strategic to military mobility - being disrupted by foreign actors, which could lead to cascade effects on the Union economy. Disruptions could occur through physical, cyber or hybrid attacks, including the sabotage of entire facilities or their parts or subcomponents. They could also be linked to ICT supply chains, which underly critical components or services to critical infrastructures. _____ 1. Joint Communication to the European Parliament and the Council, Strengthening EU economic security, 3 December 2025, JOIN(2025) 977 final.	data. It also underlined the risk of the Union's critical infrastructure - including critical transport, space systems, energy and communications infrastructure, in particular those that are identified as strategic to military mobility - being disrupted by foreign actors, which could lead to cascade effects on the Union economy. Disruptions could occur through physical, cyber or hybrid attacks, including the sabotage of entire facilities or their parts or subcomponents. They could also be linked to ICT supply chains, which underly critical components or services to critical infrastructures. _____ 1. Joint Communication to the European Parliament and the Council, Strengthening EU economic security, 3 December 2025, JOIN(2025) 977 final.
Recital 131		
144	(131) In response to challenges to ICT supply chain security posed by non-technical risks, some Member States have taken regulatory measures, including designation of high-risk suppliers, whilst other Member States are likely to do so. This could lead to further divergence in national approaches, and ultimately to higher vulnerability of some Member States, with potential spill-over effects across the Union. Therefore, it is necessary to harmonise certain aspects related to the non-technical cybersecurity risks to the ICT supply chain. Such intervention at Union level is also justified in view of the need to ensure a high level of cybersecurity across the Union. The provisions on the ICT supply chain security aim to remove such wide divergences among Member States, in particular by setting out rules for risk assessment mechanisms of ICT supply chain security risks at Union level and minimum standards of protection from ICT supply chain risks.	(131) In response to challenges to ICT supply chain security posed by non-technical risks, some Member States have taken regulatory measures, including designation of high-risk suppliers, whilst other Member States are likely to do so. This could lead to further divergence in national approaches, and ultimately to higher vulnerability of some Member States, with potential spill-over effects across the Union. Therefore, it is necessary to harmonise certain aspects related to the non-technical cybersecurity risks to the ICT supply chain. Such intervention at Union level is also justified in view of the need to ensure a high level of cybersecurity across the Union. The provisions on the ICT supply chain security aim to remove such wide divergences among Member States, in particular by setting out rules for risk assessment mechanisms of ICT supply chain security risks at Union level and minimum standards of protection from ICT supply chain risks.
Recital 132		
145	(132) To reduce critical dependencies and vulnerabilities, it is necessary to establish a trusted ICT supply chain framework which should address non-technical risks related to high-risk suppliers and dependencies in sectors of high	(132) To reduce critical dependencies and vulnerabilities, it is necessary to establish a trusted ICT supply chain framework which should address non-technical risks related to high-risk suppliers and dependencies in sectors of high

	CLEAN Commission Proposal	VS.EC Council Mandate
	criticality and other critical sectors. Therefore, it is necessary to provide an objective, risk-based, future-proof and technology-neutral framework at Union level, to identify key ICT assets and provide for a set of proportionate mitigating measures to address the risks.	criticality and other critical sectors. Therefore, it is necessary to provide an objective, risk-based, future-proof and technology-neutral framework at Union level, to identify key ICT assets and provide for a set of proportionate mitigating measures to address the risks.
Recital 133		
146	(133) Cybersecurity risks, including risks related to dependency on high-risk suppliers may be observed in several critical ICT supply chains in the Union, including detection equipment, connected and automated vehicles, electricity supply systems and electricity storage, water supply systems, drones and counter-drones systems, cloud computing services, medical devices, surveillance equipment, space services and semiconductors. For example, vulnerabilities in security detection equipment could grant access to ICT systems allowing malicious actors to manipulate scanners in such a way that prohibited items could be brought through the security checkpoint without being detected, with possibly catastrophic consequences.	(133) Cybersecurity risks, including risks related to dependency on high-risk suppliers may be observed in several critical ICT supply chains in the Union, including detection equipment, connected and automated vehicles, electricity supply systems and electricity storage, water supply systems, drones and counter-drones systems, cloud computing services, medical devices, surveillance equipment, space services and semiconductors. For example, vulnerabilities in security detection equipment could grant access to ICT systems allowing malicious actors to manipulate scanners in such a way that prohibited items could be brought through the security checkpoint without being detected, with possibly catastrophic consequences.
Recital 134		
147	(134) This Regulation should not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity for what concerns ICT supply chain security, provided that such provisions are consistent with Member States' obligations laid down in Union law. Such provisions may for instance include imposing stricter mitigation measures as regards the key ICT assets.	(134) This Regulation should not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity for what concerns ICT supply chain security, provided that such provisions are consistent with Member States' obligations laid down in Union law. Such provisions may for instance include imposing stricter mitigation measures as regards the key ICT assets.
Recital 135		
148	(135) In order to identify potential cybersecurity risks affecting specific ICT supply chains, the Cooperation Group established by Article 14 of Directive (EU) 2022/2555 ('NIS Cooperation Group') may assess specific ICT supply chains by means of Union-level coordinated security risk assessments. The Union-level coordinated security risk assessments should look, among others, at	(135) In order to identify potential cybersecurity risks affecting specific ICT supply chains, the Cooperation Group established by Article 14 of Directive (EU) 2022/2555 ('NIS Cooperation Group') may assess specific ICT supply chains by means of Union-level coordinated security risk assessments. The Union-level coordinated security risk assessments should look, among others, at

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	the main threat actors, the main threats and vulnerabilities affecting the key ICT assets. The Union-level coordinated security risk assessments should develop a list of risk scenarios and a list of measures to mitigate the risks. Union-level coordinated security risk assessments should be completed within six months. In case of specific urgency, it should be possible to shorten the deadlines.	the main threat actors, the main threats and vulnerabilities affecting the key ICT assets. The Union-level coordinated security risk assessments should develop a list of risk scenarios and a list of measures to mitigate the risks. Union-level coordinated security risk assessments should be completed within six months. In case of specific urgency, it should be possible to shorten the deadlines.
Recital 136		
149	(136) In cases where the Commission has sufficient reason to believe that there is a significant cyber threat for the security of the Union related to critical ICT supply chains and an action might be necessary to preserve the proper functioning of the internal market, it should without delay consult Member States on the need for mitigating measures and carry out a security risk assessment, taking into account the consultation of the Member States.	(136) In cases where the Commission has sufficient reason to believe that there is a significant cyber threat for the security of the Union related to critical ICT supply chains and an action might be necessary to preserve the proper functioning of the internal market, it should without delay consult Member States on the need for mitigating measures and carry out a security risk assessment, taking into account the consultation of the Member States.
Recital 137		
150	(137) Where, as a result of a security risk assessment conducted by the NIS Cooperation Group or the Commission, it appears that a specific third country poses serious and structural non-technical cybersecurity risks to ICT supply chains, the Commission should verify the threat posed by that country. The Commission may initiate such verification also on the basis of other sources such as a public statement on behalf of the Union or a Member States in response to, instances of irresponsible state behaviour in cyberspace that has led to a cybersecurity incident. In order to assess the level of threat, the Commission should take into account elements such as the existence of laws or practices in the third country which require entities under their jurisdiction to report information on software or hardware vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited. Another relevant element is the absence of effective judicial remedies, and independent and democratic control mechanisms, that can correct security concerns, including about existing practices, the substantiated information about incidents of threat actors operating out of the territory of that country carrying out malicious cyber	(137) Where, as a result of a security risk assessment conducted by the NIS Cooperation Group or the Commission, it appears that a specific third country poses serious and structural non-technical cybersecurity risks to ICT supply chains, the Commission should verify the threat posed by that country. The Commission may initiate such verification also on the basis of other sources such as a public statement on behalf of the Union or a Member States in response to, instances of irresponsible state behaviour in cyberspace that has led to a cybersecurity incident. In order to assess the level of threat, the Commission should take into account elements such as the existence of laws or practices in the third country which require entities under their jurisdiction to report information on software or hardware vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited. Another relevant element is the absence of effective judicial remedies, and independent and democratic control mechanisms, that can correct security concerns, including about existing practices, the substantiated information about incidents of threat actors operating out of the territory of that country carrying out malicious cyber

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	activities or campaigns, and the lack of ability or willingness of the third country to cooperate with the Commission or Member States to address the risk stemming from the operation of such threat actors. The Commission should also take into account information stemming from Union-level coordinated security risk assessments or reports issued by Member States or international organisations such as NATO.	activities or campaigns, and the lack of ability or willingness of the third country to cooperate with the Commission or Member States to address the risk stemming from the operation of such threat actors. The Commission should also take into account information stemming from Union-level coordinated security risk assessments or reports issued by Member States or international organisations such as NATO.
Recital 138		
151	(138) For the purpose of this Regulation, the notion of control should be understood as the ability to exercise a decisive influence on a legal entity directly, or indirectly through one or more intermediate legal entities The control of entities from a third country posing cybersecurity concerns should also be established in situations where such entity is having executive management structures in that country.	(138) For the purpose of this Regulation, the notion of control should be understood as the ability to exercise a decisive influence on a legal entity directly, or indirectly through one or more intermediate legal entities The control of entities from a third country posing cybersecurity concerns should also be established in situations where such entity is having executive management structures in that country.
Recital 139		
152	(139) The Union should not fund projects involving high-risk suppliers, which would jeopardise the Union's security and undermine the Union's interests and credibility. High-risk suppliers identified under this Regulation should therefore not be entitled to participate in any Union funding programmes and instruments implemented in direct and indirect management in accordance with the Article 136 of the Regulation (EU/Eurotom) 2024/2509 and Union sector specific rules as well as in any Union funding activities implemented in shared management, including under the next Multiannual Financial Framework in relation to the provision of ICT components or components that include ICT components to be used in identified key ICT assets. Union implementing partners, such as European Investment Bank Group and national promotional banks and institutions should refrain from supporting projects that contradict the above, including in operations at own risk.	(139) The Union should not fund projects involving high-risk suppliers, which would jeopardise the Union's security and undermine the Union's interests and credibility. High-risk suppliers identified under this Regulation should therefore not be entitled to participate in any Union funding programmes and instruments implemented in direct and indirect management in accordance with the Article 136 of the Regulation (EU/Eurotom) 2024/2509 and Union sector specific rules as well as in any Union funding activities implemented in shared management, including under the next Multiannual Financial Framework in relation to the provision of ICT components or components that include ICT components to be used in identified key ICT assets. Union implementing partners, such as European Investment Bank Group and national promotional banks and institutions should refrain from supporting projects that contradict the above, including in operations at own risk.
Recital 140		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
153	(140) Public procurement can be a strong tool for public authorities to contribute to a more innovative, sustainable and competitive economy and for spending public money in a strategic manner. Public procurement related to ICT supply chains should not be used to benefit suppliers that threaten the security of the Union's critical infrastructure. High-risk suppliers identified under this Regulation should therefore not be entitled to participate in public procurement concerning the provision of ICT components or components that include ICT components to be used in identified key ICT assets.	(140) Public procurement can be a strong tool for public authorities to contribute to a more innovative, sustainable and competitive economy and for spending public money in a strategic manner. Public procurement related to ICT supply chains should not be used to benefit suppliers that threaten the security of the Union's critical infrastructure. High-risk suppliers identified under this Regulation should therefore not be entitled to participate in public procurement concerning the provision of ICT components or components that include ICT components to be used in identified key ICT assets.
Recital 141		
154	(141) Cybersecurity certification plays a role in strengthening overall security and countering cyber threats, serving as benchmark of trust. This trust could be eroded if cybersecurity skills attestations were delivered by high-risk suppliers that should therefore not be entitled to apply to become authorised providers of any Union individual cybersecurity skills attestations. In a similar vein, it is also appropriate to exclude high-risk suppliers from obtaining cybersecurity certification under the ECCF, and becoming accredited conformity assessment bodies to deliver such certificates.	(141) Cybersecurity certification plays a role in strengthening overall security and countering cyber threats, serving as benchmark of trust. This trust could be eroded if cybersecurity skills attestations were delivered by high-risk suppliers that should therefore not be entitled to apply to become authorised providers of any Union individual cybersecurity skills attestations. In a similar vein, it is also appropriate to exclude high-risk suppliers from obtaining cybersecurity certification under the ECCF, and becoming accredited conformity assessment bodies to deliver such certificates.
Recital 142		
155	(142) Cybersecurity standards play a critical role in the security and trustworthiness of digital infrastructures. It is necessary to take appropriate measures to ensure standardisation in the field of cybersecurity. The involvement of entities established in or controlled from countries which have been identified as posing cybersecurity concerns to the ICT supply chain in line with this Regulation may lead to influencing cybersecurity standards in a way that undermines their security and trustworthiness.	(142) Cybersecurity standards play a critical role in the security and trustworthiness of digital infrastructures. It is necessary to take appropriate measures to ensure standardisation in the field of cybersecurity. The involvement of entities established in or controlled from countries which have been identified as posing cybersecurity concerns to the ICT supply chain in line with this Regulation may lead to influencing cybersecurity standards in a way that undermines their security and trustworthiness.
Recital 143		
156	(143) Based on the results of the security risk assessments, the Commission may identify, by means of implementing acts, which ICT assets should be regarded as	(143) Based on the results of the security risk assessments, the Commission may identify, by means of implementing acts, which ICT assets should be regarded as

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	key ICT assets due to their criticality and subject to specific mitigating measures. The mere existence of the possibility of connectivity of the asset should be sufficient to consider their cybersecurity risk.	key ICT assets due to their criticality and subject to specific mitigating measures. The mere existence of the possibility of connectivity of the asset should be sufficient to consider their cybersecurity risk.
Recital 144		
157	(144) Where necessary to ensure a high level of cybersecurity, cyber resilience and trust within the Union, the mitigating measures may be applied to entities in relation to their ICT supply chain and in particular to key ICT assets identified. The proposed mitigating measures should be based on the assessment of potential risks and dependencies, including the potential economic and societal impact of such measures on the entities concerned operating in highly critical or other critical sectors and in particular SMEs. The economic impact should look at the costs of the implementation of the mitigation measures, including the duration of the lifecycle of the relevant components in the key ICT assets in case where the measures include the replacement of suppliers. The availability of alternative suppliers on the market should also be assessed in order to ensure continued provision of the services.	(144) Where necessary to ensure a high level of cybersecurity, cyber resilience and trust within the Union, the mitigating measures may be applied to entities in relation to their ICT supply chain and in particular to key ICT assets identified. The proposed mitigating measures should be based on the assessment of potential risks and dependencies, including the potential economic and societal impact of such measures on the entities concerned operating in highly critical or other critical sectors and in particular SMEs. The economic impact should look at the costs of the implementation of the mitigation measures, including the duration of the lifecycle of the relevant components in the key ICT assets in case where the measures include the replacement of suppliers. The availability of alternative suppliers on the market should also be assessed in order to ensure continued provision of the services.
Recital 145		
158	(145) As mitigating measures could potentially have a restrictive effect on international trade in goods and services, they should be proportionate and targeted to pursue the legitimate objective to ensure the cybersecurity of ICT supply chains in relation to entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555, in line with the Union's international obligations.	(145) As mitigating measures could potentially have a restrictive effect on international trade in goods and services, they should be proportionate and targeted to pursue the legitimate objective to ensure the cybersecurity of ICT supply chains in relation to entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555, in line with the Union's international obligations.
Recital 146		
159	(146) Use, installation or any other kind of integration of components provided by high-risk suppliers in the operation of key ICT assets may be related to risks of subsequent transfers of data to a third country. In particular, risks may be posed by an insufficient level of protection offered to the data in the third country, such as for the protection of fundamental rights, intellectual property or trade secrets,	(146) Use, installation or any other kind of integration of components provided by high-risk suppliers in the operation of key ICT assets may be related to risks of subsequent transfers of data to a third country. In particular, risks may be posed by an insufficient level of protection offered to the data in the third country, such as for the protection of fundamental rights, intellectual property or trade secrets,

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	or unlawful access and exploitation of that data for possible future supply chain disruptions and espionage purposes. To mitigate such risks, restrictions in relation to transfer of specific types of data to third countries may be applied.	or unlawful access and exploitation of that data for possible future supply chain disruptions and espionage purposes. To mitigate such risks, restrictions in relation to transfer of specific types of data to third countries may be applied.
Recital 147		
160	(147) Important vulnerabilities stem from a lack of diversity in equipment used by entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555. A reliance on a single supplier creates a dependency on specific equipment or solutions. A lack of diversity of suppliers increases the overall vulnerability of critical infrastructure, in particular if entities source their ICT components used in sensitive ICT assets from a supplier presenting a high degree of risk. Dependency also significantly affects national and Union-wide resilience and creates single points of failure. To mitigate such risks, requirements to have more than one supplier for specific key ICT assets may be applied.	(147) Important vulnerabilities stem from a lack of diversity in equipment used by entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555. A reliance on a single supplier creates a dependency on specific equipment or solutions. A lack of diversity of suppliers increases the overall vulnerability of critical infrastructure, in particular if entities source their ICT components used in sensitive ICT assets from a supplier presenting a high degree of risk. Dependency also significantly affects national and Union-wide resilience and creates single points of failure. To mitigate such risks, requirements to have more than one supplier for specific key ICT assets may be applied.
Recital 148		
161	(148) Union entities may also be using key assets as defined by this Regulation. Therefore, the rules laid down in this Regulation concerning ICT supply chain security should also be applicable to them. To ensure that the specificity of Union entities is taken into account, it is important to consider non-technical risks stemming from ICT supply chains in regard to Union entities when conducting Union-level coordinated security risk assessments.	(148) Union entities may also be using key assets as defined by this Regulation. Therefore, the rules laid down in this Regulation concerning ICT supply chain security should also be applicable to them. To ensure that the specificity of Union entities is taken into account, it is important to consider non-technical risks stemming from ICT supply chains in regard to Union entities when conducting Union-level coordinated security risk assessments.
Recital 149		
162	(149) In exceptional circumstances justifying an immediate intervention to preserve the proper functioning of the internal market and where there is a clear evidence giving the Commission sufficient reason to consider that the use of ICT components or components that include ICT components from a specific supplier represents a significant cybersecurity threat for the economic or societal activities of at least three Member States, the Commission may propose, in close consultation with Member States, to prohibit the use, installation or integration	(149) In exceptional circumstances justifying an immediate intervention to preserve the proper functioning of the internal market and where there is a clear evidence giving the Commission sufficient reason to consider that the use of ICT components or components that include ICT components from a specific supplier represents a significant cybersecurity threat for the economic or societal activities of at least three Member States, the Commission may propose, in close consultation with Member States, to prohibit the use, installation or integration

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	of such components from this supplier by type of entities referred to in Annexes I and II to Directive (EU) 2022/2555.	of such components from this supplier by type of entities referred to in Annexes I and II to Directive (EU) 2022/2555.
Recital 150		
163	(150) In order to ensure proportionality of measures applied, entities established in a third country posing cybersecurity concerns designated in accordance with this Regulation, or controlled by such third country, by an entity established in such third country, or by a national of such third country can apply to be exempted from the prohibition to provide to entities of a type referred to in Annexes I and II to Directive (EU) 2022/2555 ICT components or components that include ICT components for their use, installation or integration in key ICT assets of that entity and participate in public procurement procedures organised in accordance with legislation transposing Directives 2014/24/EU[1] and 2014/25/EU of the European Parliament and of the Council[2] procedures in relation to the provision of ICT components or components that include ICT components to be used in identified key ICT assets. For that purpose, the entity should demonstrate with clear evidence that it applies effective measures addressing the non-technical risks and ensuring the absence of any possible undue interference by a third country posing cybersecurity concerns. _____ 1. Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, pp. 65–242, ELI: https://eur-lex.europa.eu/eli/dir/2014/24/oj/eng). 2. Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC (OJ L 94 du 28.3.2014, p. 243-374, ELI: https://eur-lex.europa.eu/eli/dir/2014/25/oj?locale=fr).	(150) In order to ensure proportionality of measures applied, entities established in a third country posing cybersecurity concerns designated in accordance with this Regulation, or controlled by such third country, by an entity established in such third country, or by a national of such third country can apply to be exempted from the prohibition to provide to entities of a type referred to in Annexes I and II to Directive (EU) 2022/2555 ICT components or components that include ICT components for their use, installation or integration in key ICT assets of that entity and participate in public procurement procedures organised in accordance with legislation transposing Directives 2014/24/EU[1] and 2014/25/EU of the European Parliament and of the Council[2] procedures in relation to the provision of ICT components or components that include ICT components to be used in identified key ICT assets. For that purpose, the entity should demonstrate with clear evidence that it applies effective measures addressing the non-technical risks and ensuring the absence of any possible undue interference by a third country posing cybersecurity concerns. _____ 1. Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, pp. 65–242, ELI: https://eur-lex.europa.eu/eli/dir/2014/24/oj/eng). 2. Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC (OJ L 94 du 28.3.2014, p. 243-374, ELI: https://eur-lex.europa.eu/eli/dir/2014/25/oj?locale=fr).
Recital 151		
164	(151) Electronic communications networks form the backbone for a wide range of services that are essential for the functioning of the internal market and the maintenance and operation of vital societal and economic functions – such as	(151) Electronic communications networks form the backbone for a wide range of services that are essential for the functioning of the internal market and the maintenance and operation of vital societal and economic functions – such as

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	energy, transport, banking, health, defence, as well as industrial control systems. Therefore, those highly critical networks are attractive targets for all types of cyberattacks and hybrid threats, for disruptions, espionage, intelligence gathering, as well as for fraud and financial crime. The risk assessment of the NIS Cooperation Group on the cybersecurity and resiliency of Europe's communications infrastructures and networks identified a number of risks and threats of strategic importance from a Union perspective, such as wiper/ransomware, attacks, supply chain attacks, network intrusions, and Distributed denial-of-service (DDoS) attacks.	energy, transport, banking, health, defence, as well as industrial control systems. Therefore, those highly critical networks are attractive targets for all types of cyberattacks and hybrid threats, for disruptions, espionage, intelligence gathering, as well as for fraud and financial crime. The risk assessment of the NIS Cooperation Group on the cybersecurity and resiliency of Europe's communications infrastructures and networks identified a number of risks and threats of strategic importance from a Union perspective, such as wiper/ransomware, attacks, supply chain attacks, network intrusions, and Distributed denial-of-service (DDoS) attacks.
Recital 152		
165	(152) In view of the interconnection and interdependence between the different national electronic communications networks, it is necessary that all Member States take appropriate measures to ensure the security of their networks. For the same reasons, there is a need to have in place an effective legal framework at Union level addressing also non-technical risks and ensuring the security of interconnected electronic communications networks in a comprehensive way.	(152) In view of the interconnection and interdependence between the different national electronic communications networks, it is necessary that all Member States take appropriate measures to ensure the security of their networks. For the same reasons, there is a need to have in place an effective legal framework at Union level addressing also non-technical risks and ensuring the security of interconnected electronic communications networks in a comprehensive way.
Recital 153		
166	(153) In particular, the cybersecurity of 5G networks is a matter of strategic importance for the Union as those networks form the backbone for a wide range of services of essential importance for the functioning of the internal market and are also key in setting up our defence readiness, including in relation to military mobility. 5G networks are capable of providing reliable ultra-fast connectivity, for example for data and information sharing, detection of drones and real-time battlefield coordination.	(153) In particular, the cybersecurity of 5G networks is a matter of strategic importance for the Union as those networks form the backbone for a wide range of services of essential importance for the functioning of the internal market and are also key in setting up our defence readiness, including in relation to military mobility. 5G networks are capable of providing reliable ultra-fast connectivity, for example for data and information sharing, detection of drones and real-time battlefield coordination.
Recital 154		
167	(154) 5G deployment consists primarily in non-standalone networks, where only the radio access network is upgraded to 5G technology, while the rest of the network still relies on an existing 4G core network. 5G non-standalone networks	(154) 5G deployment consists primarily in non-standalone networks, where only the radio access network is upgraded to 5G technology, while the rest of the network still relies on an existing 4G core network. 5G non-standalone networks

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	builds primarily on infrastructure already in place, meaning that the security of future 5G networks is, to a certain extent, determined by network equipment already in place and the configuration of such equipment. Therefore, mitigating measures should also cover 4G networks on which the 5G deployment relies.	builds primarily on infrastructure already in place, meaning that the security of future 5G networks is, to a certain extent, determined by network equipment already in place and the configuration of such equipment. Therefore, mitigating measures should also cover 4G networks on which the 5G deployment relies.
Recital 155		
168	(155) In order to address important security challenges in 5G networks, Member States within the NIS Cooperation Group, together with the Commission and ENISA, carried out a Union-level coordinated security risk assessment of 5G networks, examining both technical and non-technical risks. This assessment identified several risks, including potential interference from third countries or third country actors via the supply chain, and categorised assets according to their criticality. This assessment should be taken as a basis for defining the key ICT assets for 5G communications networks.	(155) In order to address important security challenges in 5G networks, Member States within the NIS Cooperation Group, together with the Commission and ENISA, carried out a Union-level coordinated security risk assessment of 5G networks, examining both technical and non-technical risks. This assessment identified several risks, including potential interference from third countries or third country actors via the supply chain, and categorised assets according to their criticality. This assessment should be taken as a basis for defining the key ICT assets for 5G communications networks.
Recital 156		
169	(156) To mitigate the risks identified in the Union-level coordinated security risk assessment of 5G networks, the NIS Cooperation Group adopted the EU Toolbox on 5G cybersecurity, setting out strategic and technical measures. Even though a majority of the Member States have legal frameworks that allow for restrictions or exclusions of high-risk suppliers as recommended in the 5G Toolbox, the implementation of those frameworks has not been uniform. This results in an important number of 5G sites across the Union being supplied by high-risk suppliers as referred to in the Commission's communication on the implementation of the 5G Toolbox[1]. This situation creates vulnerabilities, including strategic dependency and potential exposure to third-country interference, which could also affect future 6G infrastructure built on existing 5G networks. The fragmented implementation of the 5G Toolbox recommended measures, particularly regarding the scope of restrictions on high-risk suppliers, has led to divergences between Member States, which results in an unlevelled playing field that divides the internal market and weakens overall network	(156) To mitigate the risks identified in the Union-level coordinated security risk assessment of 5G networks, the NIS Cooperation Group adopted the EU Toolbox on 5G cybersecurity, setting out strategic and technical measures. Even though a majority of the Member States have legal frameworks that allow for restrictions or exclusions of high-risk suppliers as recommended in the 5G Toolbox, the implementation of those frameworks has not been uniform. This results in an important number of 5G sites across the Union being supplied by high-risk suppliers as referred to in the Commission's communication on the implementation of the 5G Toolbox[1]. This situation creates vulnerabilities, including strategic dependency and potential exposure to third-country interference, which could also affect future 6G infrastructure built on existing 5G networks. The fragmented implementation of the 5G Toolbox recommended measures, particularly regarding the scope of restrictions on high-risk suppliers, has led to divergences between Member States, which results in an unlevelled playing field that divides the internal market and weakens overall network

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	security. The European Court of Auditors has highlighted these disparities, warning that the absence of a coordinated approach undermines the functioning of the internal market. Persistent dependency on high-risk suppliers poses serious risks to the security of critical infrastructure in the Union and could erode trust in the internal market, as inconsistent security levels may discourage consumers and businesses from relying on 5G-based products and services across the Union. It is therefore essential to have Union-level measures to ensure a harmonised approach to the security of 5G networks. _____ 1. Communication from the Commission on the implementation of the 5G cybersecurity Toolbox, 15 June 2023, C(2023) 4049 final.	security. The European Court of Auditors has highlighted these disparities, warning that the absence of a coordinated approach undermines the functioning of the internal market. Persistent dependency on high-risk suppliers poses serious risks to the security of critical infrastructure in the Union and could erode trust in the internal market, as inconsistent security levels may discourage consumers and businesses from relying on 5G-based products and services across the Union. It is therefore essential to have Union-level measures to ensure a harmonised approach to the security of 5G networks. _____ 1. Communication from the Commission on the implementation of the 5G cybersecurity Toolbox, 15 June 2023, C(2023) 4049 final.
Recital 157		
170	(157) For the purpose of setting up a phasing out period for the key ICT assets of fixed and satellite electronic communications networks, the Commission should carry out an assessment taking due account of the degree of the security risks related to each specific ICT key assets of the fixed and satellite networks, the lifetime of relevant components and the economic impact that the removal of those components would have on the operators concerned. Based on the results of that assessment, the Commission may consider setting up different phasing out periods for the particular key ICT assets and their integral elements.	(157) For the purpose of setting up a phasing out period for the key ICT assets of fixed and satellite electronic communications networks, the Commission should carry out an assessment taking due account of the degree of the security risks related to each specific ICT key assets of the fixed and satellite networks, the lifetime of relevant components and the economic impact that the removal of those components would have on the operators concerned. Based on the results of that assessment, the Commission may consider setting up different phasing out periods for the particular key ICT assets and their integral elements.
Recital 158		
171	(158) For the purposes of effective supervision and enforcement of obligations concerning the providers of mobile, fixed and satellite electronic communication networks, the relevant competent authorities under this Regulation should ensure close cooperation with the competent authorities under the [DNA proposal]. Upon request from a competent authority designated under this Regulation, national regulatory authorities or other competent authorities for radio spectrum, where appropriate, should withdraw the rights referred to in Article 9 and Article 20 [DNA Proposal] if the provider of public electronic	(158) For the purposes of effective supervision and enforcement of obligations concerning the providers of mobile, fixed and satellite electronic communication networks, the relevant competent authorities under this Regulation should ensure close cooperation with the competent authorities under the [DNA proposal]. Upon request from a competent authority designated under this Regulation, national regulatory authorities or other competent authorities for radio spectrum, where appropriate, should withdraw the rights referred to in Article 9 and Article 20 [DNA Proposal] if the provider of public electronic

	CLEAN Commission Proposal	VS.EC Council Mandate
	communications networks is not complying with the obligations under this Regulation, including if the provider does not phase out ICT components or components that include ICT components from high-risk suppliers in the operation of key ICT assets within the period specified in accordance with this Regulation.	communications networks is not complying with the obligations under this Regulation, including if the provider does not phase out ICT components or components that include ICT components from high-risk suppliers in the operation of key ICT assets within the period specified in accordance with this Regulation.
Recital 159		
172	(159) In view of the differences in national governance structures, Member States should designate or establish one or more competent authorities responsible for the supervisory and enforcement measures under this Regulation.	(159) In view of the differences in national governance structures, Member States should designate or establish one or more competent authorities responsible for the supervisory and enforcement measures under this Regulation.
Recital 160		
173	(160) The competent authorities should provide support to entities of the type referred to in Annexes I and II o Directive (EU) 2022/2555 for the compliance with their obligations under this Regulation. For that purpose, the Commission should assess whether suppliers that may be affected by specific prohibitions are established in third country posing cybersecurity concerns or controlled by such third country or by an entity established in such third country or by a national of such third country. Competent authorities should cooperate closely with the Commission and other competent authorities within the Network established under this Regulation. Based on the assessment by the Commission, the competent authorities should share relevant information concerning high-risk suppliers with relevant entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555. Entities are not expected to verify whether a supplier is under foreign control but may rely fully on information received from competent authorities. The competent authorities should ensure that no unnecessary administrative burden is imposed on those entities.	(160) The competent authorities should provide support to entities of the type referred to in Annexes I and II o Directive (EU) 2022/2555 for the compliance with their obligations under this Regulation. For that purpose, the Commission should assess whether suppliers that may be affected by specific prohibitions are established in third country posing cybersecurity concerns or controlled by such third country or by an entity established in such third country or by a national of such third country. Competent authorities should cooperate closely with the Commission and other competent authorities within the Network established under this Regulation. Based on the assessment by the Commission, the competent authorities should share relevant information concerning high-risk suppliers with relevant entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555. Entities are not expected to verify whether a supplier is under foreign control but may rely fully on information received from competent authorities. The competent authorities should ensure that no unnecessary administrative burden is imposed on those entities.
Recital 161		
174	(161) In order to ensure effective compliance, this Regulation should provide for supervisory and enforcement measures through which the competent authorities	(161) In order to ensure effective compliance, this Regulation should provide for supervisory and enforcement measures through which the competent authorities

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	can supervise entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555. Where the competent authorities execute their supervisory and enforcement tasks in relation to those entities, they should not go beyond what is necessary and be proportionate to the identified risks.	can supervise entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555. Where the competent authorities execute their supervisory and enforcement tasks in relation to those entities, they should not go beyond what is necessary and be proportionate to the identified risks.
Recital 162		
175	(162) In order to make enforcement effective and consistent across the Union, it is necessary to provide enforcement powers that competent authorities can exercise for breach of the obligations laid down in this Regulation. When exercising those enforcement powers, the competent authorities should have due regard to a number of factors, including the nature, gravity and duration of the infringement, the material or non-material damage caused, whether the infringement was intentional or negligent, actions taken to prevent or mitigate the material or non-material damage, the degree of responsibility or any relevant previous infringements, the degree of cooperation with the competent authority and any other aggravating or mitigating factor. The enforcement measures, including penalties, should be proportionate and their imposition should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of defence.	(162) In order to make enforcement effective and consistent across the Union, it is necessary to provide enforcement powers that competent authorities can exercise for breach of the obligations laid down in this Regulation. When exercising those enforcement powers, the competent authorities should have due regard to a number of factors, including the nature, gravity and duration of the infringement, the material or non-material damage caused, whether the infringement was intentional or negligent, actions taken to prevent or mitigate the material or non-material damage, the degree of responsibility or any relevant previous infringements, the degree of cooperation with the competent authority and any other aggravating or mitigating factor. The enforcement measures, including penalties, should be proportionate and their imposition should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of defence.
Recital 163		
176	(163) It is important to also provide for the power to impose periodic penalty payments, in order to compel an entity of the type referred to in Annexes I or II to Directive (EU) 2022/2555 to cease an infringement of this Regulation in accordance with a prior decision of the competent authority.	(163) It is important to also provide for the power to impose periodic penalty payments, in order to compel an entity of the type referred to in Annexes I or II to Directive (EU) 2022/2555 to cease an infringement of this Regulation in accordance with a prior decision of the competent authority.
Recital 164		
177	(164) In order to ensure effective enforcement of the obligations laid down in this Regulation, each competent authority should have the power to impose or	(164) In order to ensure effective enforcement of the obligations laid down in this Regulation, each competent authority should have the power to impose or

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	request the imposition of penalties.	request the imposition of penalties.
Recital 165		
178	(165) For the purpose of imposing penalties on an entity of the type referred to in Annexes I and II to Directive (EU) 2022/2555 that is an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU. Where a fine is imposed on a person that is not an undertaking, the competent authority should take account of the general level of income in the Member State as well as the economic situation of the person when considering the appropriate amount of the penalties. It should be for the Member States to determine whether and to what extent public authorities should be subject to penalties. Imposing a penalty should not affect the application of other powers of the competent authorities.	(165) For the purpose of imposing penalties on an entity of the type referred to in Annexes I and II to Directive (EU) 2022/2555 that is an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU. Where a fine is imposed on a person that is not an undertaking, the competent authority should take account of the general level of income in the Member State as well as the economic situation of the person when considering the appropriate amount of the penalties. It should be for the Member States to determine whether and to what extent public authorities should be subject to penalties. Imposing a penalty should not affect the application of other powers of the competent authorities.
Recital 166		
179	(166) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission in respect of the adoption of implementing acts laying down detailed rules relating to fees levied by ENISA, implementing acts providing for a European cybersecurity certification scheme for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities, implementing acts laying down common principles and reference provisions intended to provide for elements across European cybersecurity certification schemes, implementing acts specifying procedures for prior approval or general delegation models, implementing acts on recognising a third country or international organisation cybersecurity certificates as equivalent to European cybersecurity certificates, implementing acts establishing a plan for peer review, implementing acts to establish the procedures, including on cross-border cooperation, for authorisation of the conformity assessment bodies, implementing acts to establish the circumstances, formats and procedures for notifications of conformity assessment bodies, implementing acts designating a third country as a country	(166) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission in respect of the adoption of implementing acts laying down detailed rules relating to fees levied by ENISA, implementing acts providing for a European cybersecurity certification scheme for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities, implementing acts laying down common principles and reference provisions intended to provide for elements across European cybersecurity certification schemes, implementing acts specifying procedures for prior approval or general delegation models, implementing acts on recognising a third country or international organisation cybersecurity certificates as equivalent to European cybersecurity certificates, implementing acts establishing a plan for peer review, implementing acts to establish the procedures, including on cross-border cooperation, for authorisation of the conformity assessment bodies, implementing acts to establish the circumstances, formats and procedures for notifications of conformity assessment bodies, implementing acts designating a third country as a country

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	posing cybersecurity concerns to ICT supply chains, implementing acts identifying key ICT assets used for the manufacturing of products or the provision of services by entities of the type referred to Annexes I and II to Directive (EU) 2022/2555, implementing acts establishing that entities operating in sectors of high criticality and other critical sectors are subject to specific mitigating measures and specifying the time periods for the phasing out of ICT components or components that include ICT components provided by high-risk suppliers, implementing acts further specifying conditions regarding the exemption for entities established in or controlled by entities from a third country posing cybersecurity concerns, as well as the adoption of implementing acts laying down detailed rules relating to fees levied by the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council, and the examination procedure should be used. In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should also be conferred on the Commission in respect of establishing a list of high-risk suppliers relevant for certain measures provided for in this Regulation.	posing cybersecurity concerns to ICT supply chains, implementing acts identifying key ICT assets used for the manufacturing of products or the provision of services by entities of the type referred to Annexes I and II to Directive (EU) 2022/2555, implementing acts establishing that entities operating in sectors of high criticality and other critical sectors are subject to specific mitigating measures and specifying the time periods for the phasing out of ICT components or components that include ICT components provided by high-risk suppliers, implementing acts further specifying conditions regarding the exemption for entities established in or controlled by entities from a third country posing cybersecurity concerns, as well as the adoption of implementing acts laying down detailed rules relating to fees levied by the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council, and the examination procedure should be used. In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should also be conferred on the Commission in respect of establishing a list of high-risk suppliers relevant for certain measures provided for in this Regulation.
Recital 167		
180	(167) It is necessary that European cybersecurity certification schemes reflect the latest technological developments, new related threats, and the adoption of new Union legislation setting out the demonstration of compliance and the presumption of conformity through European cybersecurity certification with relevant cybersecurity requirements of that legislation. For these reasons, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in order to add or modify the security objectives that European cybersecurity certification schemes pursue. Similarly, in the interests of a trusted ICT supply chain framework, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to amend Annex II to this Regulation in order to adapt it to technological developments. It is of particular	(167) It is necessary that European cybersecurity certification schemes reflect the latest technological developments, new related threats, and the adoption of new Union legislation setting out the demonstration of compliance and the presumption of conformity through European cybersecurity certification with relevant cybersecurity requirements of that legislation. For these reasons, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in order to add or modify the security objectives that European cybersecurity certification schemes pursue. Similarly, in the interests of a trusted ICT supply chain framework, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to amend Annex II to this Regulation in order to adapt it to technological developments. It is of particular

	CLEAN Commission Proposal	VS.EC Council Mandate
	importance that the Commission carry out 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. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council should receive all documents at the same time as Member States' experts, and their experts should systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.	importance that the Commission carry out 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. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council should receive all documents at the same time as Member States' experts, and their experts should systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.
Recital 168		
181	(168) ENISA's operations should be subject to regular and independent evaluation. That evaluation should have regard to ENISA's objectives, and the relevance of its tasks, in particular its tasks relating to the operational cooperation at Union level. In the event of a review, the Commission should evaluate how ENISA's role as a reference point for advice and expertise can be reinforced.	(168) ENISA's operations should be subject to regular and independent evaluation. That evaluation should have regard to ENISA's objectives, and the relevance of its tasks, in particular its tasks relating to the operational cooperation at Union level. In the event of a review, the Commission should evaluate how ENISA's role as a reference point for advice and expertise can be reinforced.
Recital 169		
182	(169) Commission Implementing Regulation (EU) 2024/482 lays down rules as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC). The EUCC is the first and only European cybersecurity certification scheme adopted under Regulation (EU) 2019/881. It concerns the certification of ICT products, including products belonging to the technical domains 'smart cards and similar devices' and 'hardware devices with security boxes', and protection profiles (as ICT processes). It is therefore necessary to ensure the continuation of certification activities as well as of the Agency's activities.	(169) Commission Implementing Regulation (EU) 2024/482 lays down rules as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC). The EUCC is the first and only European cybersecurity certification scheme adopted under Regulation (EU) 2019/881. It concerns the certification of ICT products, including products belonging to the technical domains 'smart cards and similar devices' and 'hardware devices with security boxes', and protection profiles (as ICT processes). It is therefore necessary to ensure the continuation of certification activities as well as of the Agency's activities.
Recital 170		
183	(170) The European Data Protection Supervisor and the European Data Protection Board were consulted in accordance with Article 42(2) of Regulation (EU) 2018/1725[1] and delivered a joint opinion [date].	(170) The European Data Protection Supervisor and the European Data Protection Board were consulted in accordance with Article 42(2) of Regulation (EU) 2018/1725[1] and delivered a joint opinion [date].

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	_____ 1. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).	_____ 1. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).
Recital 171		
184	(171) Regulation (EU) 2019/881 should be repealed.	(171) Regulation (EU) 2019/881 should be repealed.
Recital 172		
185	(172) Since the objectives 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 (TEU). 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 those objectives,	(172) Since the objectives 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 (TEU). 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 those objectives,
Formula		
186	HAVE ADOPTED THIS REGULATION:	HAVE ADOPTED THIS REGULATION:
TITLE I		
187	TITLE I GENERAL PROVISIONS	TITLE I GENERAL PROVISIONS
Article 1		
188	Article 1 Subject matter and scope	Article 1 Subject matter and scope Suggestion to come back after the whole read-through of the CSA 2.
Article 1(1)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
189	1. This Regulation lays down:	1. This Regulation lays down:
Article 1(1), point (a)		
190	(a) the mission, objectives, tasks and organisational matters relating to the European Union Agency for Cybersecurity (ENISA);	(a) the mission, objectives, tasks and organisational matters relating to the European Union Agency for Cybersecurity (ENISA);
Article 1(1), point (b)		
191	(b) a framework for establishing European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services, ICT processes, managed security services or the cybersecurity posture of entities 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; and	(b) a framework for establishing European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services, ICT processes, managed security services or the cybersecurity posture of entities 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; and
Article 1(1), point (c)		
192	(c) a trusted ICT supply chain framework.	(c) a trusted ICT supply chain framework.
Article 1(2)		
193	2. The framework referred to in paragraph 1, point (b) applies without prejudice to specific provisions in other Union legal acts regarding voluntary or mandatory certification.	2. The framework referred to in paragraph 1, point (b) applies without prejudice to specific provisions in other Union legal acts regarding voluntary or mandatory certification.
Article 1(3)		
194	3. The framework referred to in the first subparagraph point (c) shall apply to public or private entities of a type referred to in Annex I or II to Directive (EU) 2022/2555 which provide their services or carry out their activities within the Union.	3. The framework referred to in the first subparagraph point (c) shall apply to public or private entities of a type referred to in Annex I or II to Directive (EU) 2022/2555 which provide their services or carry out their activities within the Union.
Article 1(4)		
195	4. This Regulation is without prejudice to the Member States' essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security	4. This Regulation is without prejudice to the Member States' essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	remains the sole responsibility of each Member State.	remains the sole responsibility of each Member State.
Article 2		
196	Article 2 Definitions	Article 2 Definitions Suggestion to come back after the whole read-through of the CSA 2.
Article 2, first paragraph		
197	For the purposes of this Regulation, the following definitions apply:	For the purposes of this Regulation, the following definitions apply:
Article 2, first paragraph, point (1)		
198	(1) 'cybersecurity' means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats;	(1) 'cybersecurity' means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats; Definition of 'cybersecurity' to be revisited? To take into consideration the impact on other legislations that refer to this definition. Drafting suggestion from the Presidency in order to make the definition more current and updated with the continuously evolving cyber environment: 'Cybersecurity' is the safeguarding of people, society, organizations and nations from cyber risks. It's the preservation of confidentiality, availability and integrity of Information in the Cyberspace. 'Cyberspace' is a complex (virtual) environment resulting from the interaction of people, software, services on the Internet, enabled by technology devices and networks connected to it and are considered part of it. It should be explained in a recital that the terms safeguarding/preservation refer to the actions/measures/activities taken to keep cyber risk at a tolerable level. Also, in the recital it should be added that cybersecurity is, among others, a collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurance,

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
		technologies that can be used to protect the cyber environment and organization, and its key assets.
Article 2, first paragraph, point (2)		
199	(2) 'Union entities' means Union entities as defined in Article 3, point (1), of Regulation (EU, Euratom) 2023/2841;	(2) 'Union entities' means Union entities as defined in Article 3, point (1), of Regulation (EU, Euratom) 2023/2841;
Article 2, first paragraph, point (3)		
200	(3) 'authorised attestation provider' means an entity, public or private, for which ENISA has adopted a decision authorising that entity to award European individual cybersecurity skills attestations as laid down in a European individual cybersecurity skills attestation scheme;	(3) 'authorised attestation provider' means an entity, public or private, for which ENISA has adopted a decision authorising that entity to award European individual cybersecurity skills attestations as laid down in a European individual cybersecurity skills attestation scheme;
Article 2, first paragraph, point (4)		
201	(4) 'European individual cybersecurity skills attestation' means a record, in digital or physical form, attesting that an individual knows, understands and is able to perform the tasks associated to a role profile or a subset of a role profile of the European Cybersecurity Skills Framework ('ECSF'), following an assessment as laid down in a European individual cybersecurity skills attestation scheme;	(4) 'European individual cybersecurity skills attestation' means a record, in digital or physical form, attesting that an individual knows, understands and is able to perform the tasks associated to a role profile or a subset of a role profile of the European Cybersecurity Skills Framework ('ECSF'), following an assessment as laid down in a European individual cybersecurity skills attestation scheme;
Article 2, first paragraph, point (5)		
202	(5) 'European individual cybersecurity skills attestation scheme' means a comprehensive set of rules, requirements, standards and procedures established by ENISA and associated to a role profile of the ECSF or a subset thereof, and that apply to and are applied by authorised attestation providers;	(5) 'European individual cybersecurity skills attestation scheme' means a comprehensive set of rules, requirements, standards and procedures established by ENISA and associated to a role profile of the ECSF or a subset thereof, and that apply to and are applied by authorised attestation providers;
Article 2, first paragraph, point (6)		
203	(6) 'network and information system' means a network and information system as defined in Article 6, point (1), of Directive (EU) 2022/2555;	(6) 'network and information system' means a network and information system as defined in Article 6, point (1), of Directive (EU) 2022/2555;
Article 2, first paragraph, point (7)		
204	(7) 'national cybersecurity strategy' means a national cybersecurity strategy as	(7) 'national cybersecurity strategy' means a national cybersecurity strategy as

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	defined in Article 6, point (4), of Directive (EU) 2022/2555;	defined in Article 6, point (4), of Directive (EU) 2022/2555;
Article 2, first paragraph, point (8)		
205	(8) 'incident' means an incident as defined in Article 6, point (6), of Directive (EU) 2022/2555;	(8) 'incident' means an incident as defined in Article 6, point (6), of Directive (EU) 2022/2555;
Article 2, first paragraph, point (9)		
206	(9) 'large-scale cybersecurity incident' means a large-scale cybersecurity incident as defined in Article 6, point (7), of Directive (EU) 2022/2555;	(9) 'large-scale cybersecurity incident' means a large-scale cybersecurity incident as defined in Article 6, point (7), of Directive (EU) 2022/2555;
Article 2, first paragraph, point (10)		
207	(10) 'incident handling' means incident handling as defined in Article 6, point (8), of Directive (EU) 2022/2555;	(10) 'incident handling' means incident handling as defined in Article 6, point (8), of Directive (EU) 2022/2555;
Article 2, first paragraph, point (11)		
208	(11) 'cyber threat' means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons;	(11) 'cyber threat' means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons;
Article 2, first paragraph, point (12)		
209	(12) '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, managed security services or cyber posture of entities;	(12) '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, managed security services or cyber posture of entities;
Article 2, first paragraph, point (13)		
210	(13) '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, managed security services or cyber posture of entities falling under the scope of the specific scheme;	(13) '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, managed security services or cyber posture of entities falling under the scope of the specific scheme;

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 2, first paragraph, point (14)		
211	(14) 'European cybersecurity certificate' means a document issued by a relevant body, attesting that a given ICT product, ICT service, ICT process or managed security services, or the cyber posture of an entity has been evaluated for compliance with specific security requirements laid down in a European cybersecurity certification scheme;	(14) 'European cybersecurity certificate' means a document issued by a relevant body, attesting that a given ICT product, ICT service, ICT process or managed security services, or the cyber posture of an entity has been evaluated for compliance with specific security requirements laid down in a European cybersecurity certification scheme;
Article 2, first paragraph, point (15)		
212	(15) 'EU statement of conformity' means a document issued by a manufacturer or provider of ICT products, ICT services, ICT processes, managed security services or the entity the cyber posture of which is subject to certification, stating that the fulfilment of the requirements corresponding to assurance level "basic", laid down in the European cybersecurity certification scheme, has been demonstrated through conformity self-assessment;	(15) 'EU statement of conformity' means a document issued by a manufacturer or provider of ICT products, ICT services, ICT processes, managed security services or the entity the cyber posture of which is subject to certification, stating that the fulfilment of the requirements corresponding to assurance level "basic", laid down in the European cybersecurity certification scheme, has been demonstrated through conformity self-assessment;
Article 2, first paragraph, point (16)		
213	(16) 'ICT product' means an element or a group of elements of a network or information system;	(16) 'ICT product' means an element or a group of elements of a network or information system;
Article 2, first paragraph, point (17)		
214	(17) 'ICT service' means a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems;	(17) 'ICT service' means a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems;
Article 2, first paragraph, point (18)		
215	(18) 'ICT process' means a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service;	(18) 'ICT process' means a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service;
Article 2, first paragraph, point (19)		
216	(19) 'managed security service' means a service provided to a third party consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, such as incident handling, penetration testing,	(19) 'managed security service' means a service provided to a third party consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, such as incident handling, penetration testing,

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	security audits and consulting, including expert advice related to technical support;	security audits and consulting, including expert advice related to technical support;
Article 2, first paragraph, point (20)		
217	(20) 'accreditation' means accreditation as defined in Article 2, point (10), of Regulation (EC) No 765/2008;	(20) 'accreditation' means accreditation as defined in Article 2, point (10), of Regulation (EC) No 765/2008;
Article 2, first paragraph, point (21)		
218	(21) 'national accreditation body' means a national accreditation body as defined in Article 2, point (11), of Regulation (EC) No 765/2008;	(21) 'national accreditation body' means a national accreditation body as defined in Article 2, point (11), of Regulation (EC) No 765/2008;
Article 2, first paragraph, point (22)		
219	(22) 'conformity assessment' means a conformity assessment as defined in Article 2, point (12), of Regulation (EC) No 765/2008;	(22) 'conformity assessment' means a conformity assessment as defined in Article 2, point (12), of Regulation (EC) No 765/2008;
Article 2, first paragraph, point (23)		
220	(23) 'conformity assessment body' means a conformity assessment body as defined in Article 2, point (13), of Regulation (EC) No 765/2008;	(23) 'conformity assessment body' means a conformity assessment body as defined in Article 2, point (13), of Regulation (EC) No 765/2008;
Article 2, first paragraph, point (24)		
221	(24) 'standard' means a standard as defined in Article 2, point (1), of Regulation (EU) No 1025/2012 of the European Parliament and of the Council[1]; _____ 1. Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).	(24) 'standard' means a standard as defined in Article 2, point (1), of Regulation (EU) No 1025/2012 of the European Parliament and of the Council[1]; _____ 1. Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).
Article 2, first paragraph, point (25)		
222	(25) 'technical specification' means a technical specification as defined in	(25) 'technical specification' means a technical specification as defined in

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	Article 2, point (4), of Regulation (EU) No 1025/2012;	Article 2, point (4), of Regulation (EU) No 1025/2012;
Article 2, first paragraph, point (26)		
223	(26) 'harmonised standard' means a harmonised standard as defined in Article 2, point (1) (c), of Regulation (EU) No 1025/2012;	(26) 'harmonised standard' means a harmonised standard as defined in Article 2, point (1) (c), of Regulation (EU) No 1025/2012;
Article 2, first paragraph, point (27)		
224	(27) 'assurance level' means a basis for confidence that an ICT product, ICT service, ICT process, managed security service or the cyber posture of an entity meets the security requirements of a specific European cybersecurity certification scheme, and indicates the level at which an ICT product, ICT service, ICT process, managed security service or cyber posture of entity has been evaluated but as such does not measure the security of the ICT product, ICT service, ICT process, managed security service or cyber posture of entity concerned;	(27) 'assurance level' means a basis for confidence that an ICT product, ICT service, ICT process, managed security service or the cyber posture of an entity meets the security requirements of a specific European cybersecurity certification scheme, and indicates the level at which an ICT product, ICT service, ICT process, managed security service or cyber posture of entity has been evaluated but as such does not measure the security of the ICT product, ICT service, ICT process, managed security service or cyber posture of entity concerned;
Article 2, first paragraph, point (27a)		
224a		*(27a) 'protection profile' means an ICT process that specifies security requirements for a given category of ICT products, ICT services, ICT processes or managed security services, and that may be used to assess the object falling into that specific category for the purpose of their certification;*
Article 2, first paragraph, point (27b)		
224b		*(27b) 'extension profile' means the setting out of additional or specific security requirements, including, where applicable, security requirements set out in national provisions transposing Union law, and additional capabilities;*
Article 2, first paragraph, point (28)		
225	(28) 'conformity self-assessment' means an action carried out by a manufacturer or provider of ICT products, ICT services, ICT processes, managed security services or the entity the cyber posture of which is subject to certification, which evaluates whether those ICT products, ICT services, ICT processes, managed	(28) 'conformity self-assessment' means an action carried out by a manufacturer or provider of ICT products, ICT services, ICT processes, managed security services or the entity the cyber posture of which is subject to certification, which evaluates whether those ICT products, ICT services, ICT processes, managed

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	security services or cyber posture of entities meet the requirements of a specific European cybersecurity certification scheme;	security services or cyber posture of entities meet the requirements of a specific European cybersecurity certification scheme;
Article 2, first paragraph, point (29)		
226	(29) 'cyber posture of entities' means entities' level of cybersecurity with respect to the specific security requirements;	(29) 'cyber posture of entities' means entities' level of cybersecurity with respect to the specific security requirements;
Article 2, first paragraph, point (30)		
227	(30) 'prior approval model' means a model whereby a conformity assessment body may issue a European cybersecurity certificate based on the assessment by a national cybersecurity certification authority in the context of a specific certification process under a relevant scheme;	(30) 'prior approval model' means a model whereby a conformity assessment body may issue a European cybersecurity certificate based on the assessment by a national cybersecurity certification authority in the context of a specific certification process under a relevant scheme;
Article 2, first paragraph, point (31)		
228	(31) 'general delegation model' means a model whereby a conformity assessment body may issue a European cybersecurity certificate based on a delegation of certification activities by a national cybersecurity certification authority;	(31) 'general delegation model' means a model whereby a conformity assessment body may issue a European cybersecurity certificate based on a delegation of certification activities by a national cybersecurity certification authority;
Article 2, first paragraph, point (32)		
229	(32) 'computer security incident response team' or 'CSIRT' means a CSIRT designated or established pursuant to Article 10 of Directive (EU) 2022/2555.	(32) 'computer security incident response team' or 'CSIRT' means a CSIRT designated or established pursuant to Article 10 of Directive (EU) 2022/2555.
Article 2, first paragraph, point (33)		
230	(33) 'ICT components' means ICT products, ICT services or ICT processes that may be used in the operation of ICT assets;	(33) 'ICT components' means ICT products, ICT services or ICT processes that may be used in the operation of ICT assets;
Article 2, first paragraph, point (34)		
231	(34) 'ICT assets' means software or hardware assets in the network and information systems used by an entity of the type referred to in Annexes I and II to Directive (EU) 2022/2555;	(34) 'ICT assets' means software or hardware assets in the network and information systems used by an entity of the type referred to in Annexes I and II to Directive (EU) 2022/2555;
Article 2, first paragraph, point (35)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
232	(35) 'key ICT assets' means ICT assets identified in accordance with Article 102;	(35) 'key ICT assets' means ICT assets identified in accordance with Article 102;
Article 2, first paragraph, point (36)		
233	(36) 'electronic communications network' means electronic communications network as defined in Article 2, point (1), of Regulation (EU) XX/XXXX [DNA proposal];	(36) 'electronic communications network' means electronic communications network as defined in Article 2, point (1), of Regulation (EU) XX/XXXX [DNA proposal];
Article 2, first paragraph, point (37)		
234	(37) 'control' means the ability to exercise a decisive influence on a legal entity directly, or indirectly through one or more intermediate legal entities;	(37) 'control' means the ability to exercise a decisive influence on a legal entity directly, or indirectly through one or more intermediate legal entities;
Article 2, first paragraph, point (38)		
235	(38) 'establishment' means the effective exercise of activity through stable arrangements in the country where the entity has its central administration or its principal place of business;	(38) 'establishment' means the effective exercise of activity through stable arrangements in the country where the entity has its central administration or its principal place of business;
Article 2, first paragraph, point (39)		
236	(39) 'high-risk supplier' means either of the following:	(39) 'high-risk supplier' means either of the following:
Article 2, first paragraph, point (39)(a)		
237	(a) an entity established in a third country posing cybersecurity concerns designated in accordance with Article 100, or controlled by such third country, by an entity established in such third country, or by a national of such third country;	(a) an entity established in a third country posing cybersecurity concerns designated in accordance with Article 100, or controlled by such third country, by an entity established in such third country, or by a national of such third country;
Article 2, first paragraph, point (39)(b)		
238	(b) an entity designated in accordance with Article 103(7) and entities controlled by that entity;	(b) an entity designated in accordance with Article 103(7) and entities controlled by that entity;
Article 2, first paragraph, point (40)		
239	(40) 'ICT supply chain' means a sum of ICT services, ICT products and ICT	(40) 'ICT supply chain' means a sum of ICT services, ICT products and ICT

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	processes that encompass activities and actors involved at all stages upstream of a product being made available or a service being delivered on the market;	processes that encompass activities and actors involved at all stages upstream of a product being made available or a service being delivered on the market;
Article 2, first paragraph, point (41)		
240	(41) 'third country' means third country as defined in Article 3 (4) of Regulation (EU) 2023/2675 of the European Parliament and the Council[1]; _____ 1. Regulation (EU) 2023/2675 of the European Parliament and of the Council of 22 November 2023 on the protection of the Union and its Member States from economic coercion by third countries (OJ L, 2023/2675, 7.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2675/oj).	(41) 'third country' means third country as defined in Article 3 (4) of Regulation (EU) 2023/2675 of the European Parliament and the Council[1]; _____ 1. Regulation (EU) 2023/2675 of the European Parliament and of the Council of 22 November 2023 on the protection of the Union and its Member States from economic coercion by third countries (OJ L, 2023/2675, 7.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2675/oj).
Article 2, first paragraph, point (42)		
241	(42) 'non-technical risk' means the likelihood of the supplier being subject to influence by a third country with the potential to cause loss or disruption of the service provided or to compromise the product manufactured by an entity or to lead to exfiltration of data, including for the purposes of espionage or revenue generation;	(42) 'non-technical risk' means the likelihood of the supplier being subject to influence by a third country with the potential to cause loss or disruption of the service provided or to compromise the product manufactured by an entity or to lead to exfiltration of data, including for the purposes of espionage or revenue generation;
Article 2, first paragraph, point (43)		
242	(43) 'significant non-technical cybersecurity risk' means a non-technical cybersecurity risk which can be assumed to have a high likelihood to cause an incident that could lead to a severe negative impact, including by causing considerable material or non-material loss or disruption;	(43) 'significant non-technical cybersecurity risk' means a non-technical cybersecurity risk which can be assumed to have a high likelihood to cause an incident that could lead to a severe negative impact, including by causing considerable material or non-material loss or disruption;
Article 2, first paragraph, point (44)		
243	(44) 'core network functions of mobile electronic communications networks' means the central architectural element of the mobile electronic communications networks connecting major network nodes to the Internet and managing essential system functions that includes user equipment authentication, lawful interception (LI) functions, security gateways (SeGW) at the network edge, signalling security functions, roaming and session management, user and control plane data transport, access policy management, registration and authorisation of	(44) 'core network functions of mobile electronic communications networks' means the central architectural element of the mobile electronic communications networks connecting major network nodes to the Internet and managing essential system functions that includes user equipment authentication, lawful interception (LI) functions, security gateways (SeGW) at the network edge, signalling security functions, roaming and session management, user and control plane data transport, access policy management, registration and authorisation of

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	network services, storage of end-user and network data, critical network services including domain name system (DNS), interconnection with third-party mobile networks, exposure of core network functions to external applications, and the selection and management of network slices;	network services, storage of end-user and network data, critical network services including domain name system (DNS), interconnection with third-party mobile networks, exposure of core network functions to external applications, and the selection and management of network slices;
Article 2, first paragraph, point (45)		
244	(45) 'network function virtualisation (NFV) and management and network orchestration (MANO) of mobile electronic communications networks' means the software and architectural framework ensuring the lifecycle management, orchestration, and automation of virtualised network functions (VNFs), cloud-native network functions (CNFs) and the selection and management of network slices within mobile electronic communications networks;	(45) 'network function virtualisation (NFV) and management and network orchestration (MANO) of mobile electronic communications networks' means the software and architectural framework ensuring the lifecycle management, orchestration, and automation of virtualised network functions (VNFs), cloud-native network functions (CNFs) and the selection and management of network slices within mobile electronic communications networks;
Article 2, first paragraph, point (46)		
245	(46) 'radio access network (RAN) of mobile electronic communications networks' means the network connecting the mobile user equipment to the core network, including base stations (eNodeB for 4G, gNodeB for 5G), remote radio heads (RRH) and baseband units (BBU), active antenna systems (AAS), and where applicable, disaggregated RAN components such as centralised units (CU) and distributed units (DU), and the RAN intelligent controller (RIC);	(46) 'radio access network (RAN) of mobile electronic communications networks' means the network connecting the mobile user equipment to the core network, including base stations (eNodeB for 4G, gNodeB for 5G), remote radio heads (RRH) and baseband units (BBU), active antenna systems (AAS), and where applicable, disaggregated RAN components such as centralised units (CU) and distributed units (DU), and the RAN intelligent controller (RIC);
Article 2, first paragraph, point (47)		
246	(47) 'core network functions of fixed electronic communications networks' means the backbone intelligence of the network, connecting the major nodes and handling a range of essential functions, including user authentication and authorisation (AAA), lawful interception (LI) functions, domain name system (DNS) and IP addressing services (DHCP), access policy management, storage of end-user and network data, IP switching and routing, and international internet gateways (IIG);	(47) 'core network functions of fixed electronic communications networks' means the backbone intelligence of the network, connecting the major nodes and handling a range of essential functions, including user authentication and authorisation (AAA), lawful interception (LI) functions, domain name system (DNS) and IP addressing services (DHCP), access policy management, storage of end-user and network data, IP switching and routing, and international internet gateways (IIG);
Article 2, first paragraph, point (48)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
247	(48) 'network management system of fixed electronic communications networks' means all centralised platforms and software components necessary for the operation, administration, maintenance and provisioning (OAM&P) of the network and the monitoring of network-related information;	(48) 'network management system of fixed electronic communications networks' means all centralised platforms and software components necessary for the operation, administration, maintenance and provisioning (OAM&P) of the network and the monitoring of network-related information;
Article 2, first paragraph, point (49)		
248	(49) 'transport and transmission functions of fixed electronic communications networks' means all components necessary for the backhaul and aggregation of traffic across the network, including optical transport equipment, microwave links and submarine cable systems that include the underwater equipment as well as the submarine line terminal equipment (SLTE) and the physical landing station facilities;	(49) 'transport and transmission functions of fixed electronic communications networks' means all components necessary for the backhaul and aggregation of traffic across the network, including optical transport equipment, microwave links and submarine cable systems that include the underwater equipment as well as the submarine line terminal equipment (SLTE) and the physical landing station facilities;
Article 2, first paragraph, point (50)		
249	(50) 'access network of fixed electronic communications networks' means the network connecting the end-user premises to the aggregation or core network, including the optical line termination (OLT) and the optical network termination (ONT) for fibre networks; coaxial cable modem termination system (CMTS) and cable modems for coaxial cable networks, and fixed wireless access components where used as a fixed line substitute.	(50) 'access network of fixed electronic communications networks' means the network connecting the end-user premises to the aggregation or core network, including the optical line termination (OLT) and the optical network termination (ONT) for fibre networks; coaxial cable modem termination system (CMTS) and cable modems for coaxial cable networks, and fixed wireless access components where used as a fixed line substitute.
TITLE II		
250	TITLE II THE EUROPEAN UNION AGENCY FOR CYBERSECURITY	TITLE II THE EUROPEAN UNION AGENCY FOR CYBERSECURITY
Chapter I		
251	Chapter I Mission and Objectives	Chapter I Mission and Objectives
Article 3		
252	Article 3 Mission of ENISA	Article 3 Mission of ENISA

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 3(1)		
253	1. The mission of ENISA is to support Member States and Union entities in achieving a high level of cybersecurity, cyber resilience and trust within the Union.	1. The mission of ENISA is to support Member States and Union entities in achieving a high level of cybersecurity, cyber resilience and trust within the Union.
Article 3(2)		
254	2. ENISA shall act as a reference point for advice and expertise on cybersecurity for Member States, as well as for other stakeholders in the Union.	2. ENISA shall act as a ~~reference point~~ *centre of expertise* for advice and ~~expertise~~ *knowledge* on cybersecurity for Member States, as well as for other *relevant* stakeholders in the Union. *ENISA shall achieve this by virtue of its independence, the scientific and technical quality of the advice, contributions, and assistance it delivers, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out its tasks.*
Article 3(3)		
255	3. ENISA shall contribute to reducing the fragmentation of the internal market by carrying out the tasks assigned to it under this Regulation.	3. ENISA shall contribute to reducing the fragmentation of the internal market by carrying out the tasks assigned to it under this Regulation *or by other Union legal acts*.
Article 3(4)		
256	4. ENISA shall carry out the tasks assigned to it by Union legal acts.	4. ~~*ENISA shall carry out the tasks assigned to it by Union legal acts.*~~ Deleted, as merged with paragraph 3.
Article 3(5)		
257	5. ENISA shall develop its own capabilities, including technical and human capabilities and skills, necessary to perform the tasks assigned to it under this Regulation.	5. ENISA shall develop its own capabilities, including technical and human capabilities and skills, necessary to perform the tasks assigned to it under this Regulation.
Article 4		
258	Article 4 Objectives of ENISA	Article 4 Objectives of ENISA

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 4(1)		
259	1.ENISA shall be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice, contributions, and assistance it delivers, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out its tasks.	1. ~~*ENISA shall be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice, contributions, and assistance it delivers, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out its tasks.*~~ Deletion here as merged with Article 3. Moved to Article 3(2).
Article 4(2)		
260	2.ENISA shall assist Member States and, where appropriate, Union entities in implementing horizontal and sectoral Union policies and legislation related to cybersecurity, including market surveillance activities.	2.ENISA shall assist Member States and, where appropriate, Union entities in implementing horizontal and sectoral Union policies and legislation related to cybersecurity, including ***in carrying out*** market surveillance activities. The notion of "timely manner" to be explained in the corresponding recital.
Article 4(3)		
261	3.ENISA shall provide its expertise and assist the Commission in developing Union policies and legislation related to cybersecurity.	3.ENISA shall provide its expertise ***to*** and assist the Commission in developing Union policies and ~~*legislation*~~***law*** related to cybersecurity. "Law" for consistency of terminology throughout the text.
Article 4(4)		
262	4.ENISA shall support capacity-building and preparedness across the Union by assisting Member States, Union entities, through the Cybersecurity Service for the Union institutions, bodies, offices and agencies (CERT-EU) referred to in Chapter IV of Regulation (EU, Euratom) 2023/2841, and public and private stakeholders to increase the protection of their network and information systems, to develop and improve cyber resilience and response capacities.	4.ENISA shall support capacity-building and preparedness across the Union by assisting Member States, Union entities, through the Cybersecurity Service for the Union institutions, bodies, offices and agencies (CERT-EU) referred to in Chapter IV of Regulation (EU, Euratom) 2023/2841, and ***relevant*** public and private stakeholders to increase the protection of their network and information systems, to develop and improve cyber resilience and response capacities.

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
		Alignment with the wording of para 6.
Article 4(5)		
263	5.ENISA shall contribute to the implementation of the Cybersecurity Skills Academy and the growth of the cybersecurity workforce in the Union by supporting efforts to develop skills portability across the Union, including through the maintenance and uptake of the ECSF and the development, maintenance and uptake of European individual cybersecurity skills attestation schemes in accordance with Chapter II, Section 4 of this Title, and by ensuring the provision of training in accordance with Article 6(8).	5. ~~*ENISA shall contribute to the implementation of the Cybersecurity Skills Academy and the growth of the cybersecurity workforce in the Union by supporting efforts to develop skills portability across the Union, including through the maintenance and uptake of the ECSF and the development, maintenance and uptake of European individual cybersecurity skills attestation schemes in accordance with Chapter II, Section 4 of this Title, and by ensuring the provision of training in accordance with Article 6(8).*~~ Included as new 10(a).
Article 4(6)		
264	6.ENISA shall promote cooperation, including information sharing and coordination at Union level, among Member States, Union entities in accordance with Regulation (EU, Euratom) 2023/2841, and relevant private and public stakeholders on matters related to cybersecurity.	6.ENISA shall promote ***and facilitate*** cooperation, including information sharing and coordination at Union level, among Member States, Union entities in accordance with Regulation (EU, Euratom) 2023/2841, and relevant private and public stakeholders on matters related to cybersecurity.
Article 4(7)		
265	7.ENISA shall contribute to increasing cybersecurity capabilities at Union level in order to support the actions of Member States in preventing and responding to cyber threats.	7.ENISA shall contribute to increasing cybersecurity capabilities at Union level in order to support the actions of Member States in preventing and responding to cyber threats ***and incidents***. Not "cybersecurity incident", "incident" is defined in Article 2 (refers to the definition in NIS 2).
Article 4(8)		
266	8.ENISA shall support operational cooperation at Union level, including by contributing to shared situational awareness of the cyber threat and incident landscape among Member States and, in cooperation with CERT-EU, among	8.ENISA shall support ***and facilitate*** operational cooperation at Union level, including by contributing to shared situational awareness of the cyber threat and incident landscape among Member States, and, in cooperation with CERT-EU,

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	Union entities.	among Union entities. The issue of handling of information included in Article 67.
Article 4(9)		
267	9.ENISA shall closely cooperate with Europol, CSIRTs and other relevant national authorities in order to improve cybersecurity preparedness and response to ransomware incidents.	9.ENISA shall closely cooperate with ~~*Europol,*~~ CSIRTs and other relevant national authorities*, and where appropriate with Europol,* in order to improve cybersecurity preparedness and response to ~~*ransomware*~~ incidents. Ransomware is covered by Recital 37.
Article 4(10)		
268	10. ENISA shall contribute to the establishment and maintenance of a European cybersecurity certification framework in accordance with Title III of this Regulation. ENISA shall promote the use of European cybersecurity certification, with a view to avoiding the fragmentation of the internal market.	10. ENISA shall contribute to the establishment and maintenance of a European cybersecurity certification framework in accordance with Title III of this Regulation. ENISA shall promote the use of European cybersecurity certification, with a view to avoiding the fragmentation of the internal market.
Article 4(10a)		
268a		*10a. ENISA shall contribute to the implementation of the Cybersecurity Skills Academy and the growth of the cybersecurity workforce in the Union by supporting efforts to develop skills portability across the Union, including through the maintenance and uptake of the ECSF and the development, maintenance and uptake of European individual cybersecurity skills attestation schemes in accordance with Chapter II, Section 4 of this Title, and by ensuring the provision of training in accordance with Article 6(8).* Moved from point 5.
Article 4(11)		
269	11. ENISA shall contribute to the harmonisation of the digital single market by engaging in standardisation work relevant for Union policies related to cybersecurity and by developing technical specifications.	11. ENISA shall contribute to the harmonisation of the digital single market by ~~*engaging*~~*supporting Member States and the Commission* in standardisation work relevant for Union policies related to cybersecurity and by developing technical

	CLEAN Commission Proposal	VS.EC Council Mandate
		specifications.
Article 4(12)		
270	12. ENISA shall promote a high level of cybersecurity awareness among organisations and businesses.	12. ENISA shall promote a high level of cybersecurity awareness among organisations and businesses.
Chapter II		
271	Chapter II Tasks	Chapter II Tasks
Section 1		
272	Section 1 Support for implementation of Union policy and law	Section 1 Support for implementation of Union policy and law Terminology of "legislation/law" to be checked for coherence throughout the text.
Article 5		
273	Article 5 Support for implementation of Union policy and law	Article 5 Support for implementation of Union policy and law
Article 5(1)		
274	1.ENISA shall contribute to the implementation of Union policy and law by:	1.ENISA shall contribute to the implementation of Union policy and law by:
Article 5(1), point (a)		
275	(a) assisting Member States in implementing Union policy and law regarding cybersecurity consistently, including by issuing technical guidance and reports, by providing advice and sharing best practices, and by facilitating the exchange of best practices between competent authorities in this regard;	(a) assisting Member States in implementing Union policy and law regarding cybersecurity consistently, including by issuing technical guidance and reports, by providing advice and sharing best practices, and by facilitating the exchange of best practices between competent authorities in this regard; Same as Article 4(2).
Article 5(1), point (b)		
276	(b) supporting information sharing within and between sectors, in particular	(b) supporting information sharing within and between sectors, in particular

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	regarding the sectors listed in Annexes I and II to Directive (EU) 2022/2555 and products with digital elements falling within the scope of Regulation (EU) 2024/2847, by providing best practices and guidance on available tools and procedures;	regarding the sectors listed in Annexes I and II to Directive (EU) 2022/2555 and *regarding* products with digital elements falling within the scope of Regulation (EU) 2024/2847, by providing best practices and guidance on available tools and procedures;
Article 5(1), point (c)		
277	(c) at the request of the Commission, assisting Member States by providing support, such as technical guidance, including on cybersecurity risk management measures, tools for cybersecurity maturity assessment, and incident response playbooks, tailored to the sectors listed in Annexes I and II to Directive (EU) 2022/2555 or support for the implementation of secure-by-design principles for products with digital elements in line with Regulation (EU) 2024/2847, with a view to facilitating the improvement of the cybersecurity maturity levels and compliance with Union law regarding cybersecurity;	(c) ~~*at the request of the Commission,*~~ assisting Member States by providing support, such as technical guidance, including on cybersecurity risk management measures, tools for cybersecurity maturity ~~*assessment*~~*assessments*, and incident response playbooks, tailored to the sectors listed in Annexes I and II to Directive (EU) 2022/2555 or support for the implementation of secure-by-design principles for products with digital elements in line with Regulation (EU) 2024/2847, with a view to facilitating the improvement of the cybersecurity maturity levels and compliance with Union law regarding cybersecurity;
Article 5(1), point (d)		
278	(d) contributing to the work of the Cooperation Group established pursuant to Article 14(1) of Directive (EU) 2022/2555 ('NIS Cooperation Group'), the European Digital Identity Cooperation Group established pursuant to Article 46e(1) of Regulation (EU) No 910/2014, the European Cybersecurity Certification Group ('ECCG') as referred to in Article 90 of this Regulation, and the administrative cooperation group (ADCO) established pursuant to Article 52(15) of Regulation (EU) 2024/2847;	(d) contributing to the work of the Cooperation Group established pursuant to Article 14(1) of Directive (EU) 2022/2555 ('NIS Cooperation Group'), the European Digital Identity Cooperation Group established pursuant to Article 46e(1) of Regulation (EU) No 910/2014, the European Cybersecurity Certification Group ('ECCG') as referred to in Article 90 of this Regulation, and the administrative cooperation group (ADCO) established pursuant to Article 52(15) of Regulation (EU) 2024/2847;
Article 5(1), point (e)		
279	(e) assisting Member States and relevant Union entities in developing and promoting cybersecurity policies related to sustaining the general availability and integrity of the public core of the open internet;	(e) assisting Member States and relevant Union entities in developing and promoting cybersecurity policies related to sustaining the general availability and integrity of the public core of the open internet; This task will be clarified in the corresponding recital.
Article 5(1), point (f)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
280	(f) in accordance with Regulation (EU) 2024/2847, providing technical advice and support to Member States and the Commission on matters related to the implementation of that Regulation;	(f) in accordance with Regulation (EU) 2024/2847, providing technical advice and support to Member States and the Commission on matters related to the implementation of that Regulation;
Article 5(1), point (g)		
281	(g) assisting Member States in carrying out mutual assistance and in facilitating such cooperation processes for essential and important entities pursuant to [Article 37a of Directive (EU) 2022/2555];	(g) *[*assisting Member States in carrying out mutual assistance and in facilitating such cooperation processes for essential and important entities pursuant to [Article 37a of Directive (EU) 2022/2555];*]* To leave in brackets till negotiations on amendment of NIS2 is completed.
Article 5(1), point (h)		
282	(h) at the request of the European Data Protection Board, providing advice on the implementation of specific cybersecurity aspects of Union policy and law related to data protection and privacy.	(h) at the request of the European Data Protection Board *or European Data Protection Supervisor*, providing advice on the implementation of specific cybersecurity aspects of Union policy and law related to data protection and privacy.
Article 5(2)		
283	2.ENISA shall contribute to coordinated Union level cybersecurity risk assessments, including those carried out pursuant to Article 22 of Directive (EU) 2022/2555.	2.ENISA shall contribute to coordinated Union level cybersecurity risk assessments, including those carried out pursuant to Article 22 of Directive (EU) 2022/2555.
Article 5(3)		
284	3.ENISA shall issue guidelines regarding the interoperability of network and information systems used for information-sharing, including with regard to Cross-Border Cyber Hubs as referred to in Article 6(3) of Regulation (EU) 2025/38.	3.ENISA shall issue guidelines regarding the interoperability of network and information systems used for information-sharing, including with regard to Cross-Border Cyber Hubs as referred to in Article 6(3) of Regulation (EU) 2025/38.
Article 5(4)		
285	4.ENISA shall be a member of the NIS Cooperation Group pursuant to Article 14(3) of Directive (EU) 2022/2555.	4.ENISA shall be a member of the NIS Cooperation Group pursuant to Article 14(3) of Directive (EU) 2022/2555.
Article 5(5)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
286	5. At the Commission's request, ENISA shall provide expertise, technical advice, information or analysis or carry out preparatory work on specific cybersecurity matters with a view to informing the Commission's policymaking and monitoring of the implementation of Union legislation.	5. At the Commission's request, ENISA shall provide expertise, technical advice, information or analysis or carry out preparatory work on specific cybersecurity matters with a view to informing the Commission's policymaking and monitoring of the implementation of Union legislation. Further details to be provided in the recital.
Article 6		
287	Article 6 Capacity-building	Article 6 Capacity-building
Article 6, first paragraph		
288	ENISA shall assist:	ENISA shall assist:
Article 6, first paragraph, point (1)		
289	(1) Member States in their efforts to improve the prevention, detection and analysis of, and the capability to respond to cyber threats and incidents by providing them with knowledge and expertise;	(1) Member States***, at their request,*** in their efforts to improve the prevention, detection and analysis of, and the capability to respond to cyber threats and incidents by providing them with knowledge and expertise;
Article 6, first paragraph, point (2)		
290	(2) Member States, at their request, in establishing and implementing vulnerability disclosure policies on a voluntary basis;	(2) Member States, at their request, in establishing and implementing vulnerability disclosure policies on a voluntary basis;
Article 6, first paragraph, point (3)		
291	(3) in accordance with Regulation (EU, Euratom) 2023/2841, CERT-EU and the Interinstitutional Cybersecurity Board in their efforts to support Union entities in strengthening their cybersecurity, improve the prevention, detection and analysis of cyber threats and incidents as well as to improve their capabilities to respond to such cyber threats and incidents;	(3) in accordance with Regulation (EU, Euratom) 2023/2841, CERT-EU and the Interinstitutional Cybersecurity Board in their efforts to support Union entities in strengthening their cybersecurity, improve the prevention, detection and analysis of cyber threats and incidents as well as to improve their capabilities to respond to such cyber threats and incidents;
Article 6, first paragraph, point (4)		
292	(4) Member States in developing national CSIRTs, where requested pursuant to	(4) Member States in developing ~~*national*~~***their*** CSIRTs, where requested

	CLEAN Commission Proposal	VS.EC Council Mandate
	Article 10(10) of Directive (EU) 2022/2555;	pursuant to Article 10(10) of Directive (EU) 2022/2555 ***and in raising the level of CSIRTs capabilities, including by promoting dialogue and exchanges of information, with a view to ensuring that, with regard to the state of the art, each CSIRT possesses a common set of minimum capabilities and operates according to best practices***; Merged with point 7.
Article 6, first paragraph, point (5)		
293	(5) Member States in developing or updating a national cybersecurity strategy and key performance indicators for the assessment of that strategy, where requested pursuant to Article 7(4) of Directive (EU) 2022/2555, promote the dissemination of those strategies and note the progress in their implementation across the Union in order to promote best practices;	(5) Member States in developing or updating a national cybersecurity strategy and key performance indicators for the assessment of that strategy, where requested pursuant to Article 7(4) of Directive (EU) 2022/2555, promote the dissemination of those strategies and note the progress in their implementation across the Union in order to promote best practices;
Article 6, first paragraph, point (6)		
294	(6) Union institutions, at their request, in developing and reviewing Union strategies regarding cybersecurity, promoting their dissemination and tracking the progress in their implementation;	(6) Union ~~*institutions*~~***entities***, at their request, in developing and reviewing Union strategies regarding cybersecurity, promoting their dissemination and tracking the progress in their implementation;
Article 6, first paragraph, point (7)		
295	(7) national CSIRTs in raising the level of their capabilities, including by promoting dialogue and exchanges of information, with a view to ensuring that, with regard to the state of the art, each CSIRT possesses a common set of minimum capabilities and operates according to best practices;	(7) ~~*national CSIRTs in raising the level of their capabilities, including by promoting dialogue and exchanges of information, with a view to ensuring that, with regard to the state of the art, each CSIRT possesses a common set of minimum capabilities and operates according to best practices;*~~ Deletion (merged with point 4).
Article 6, first paragraph, point (8)		
296	(8) Member States, Union entities and public and private stakeholders in their efforts to assess, grow and enhance the cybersecurity workforce, including by	(8) Member States, Union entities and public and private stakeholders in their efforts to assess, grow and enhance the cybersecurity workforce, including by

	CLEAN Commission Proposal	VS.EC Council Mandate
	developing, maintaining and promoting the uptake of relevant tools, such as the ECSF and European individual cybersecurity skills attestation schemes in accordance with Section 4 of this Chapter;	developing, maintaining and promoting the uptake of relevant tools, such as the ECSF and European individual cybersecurity skills attestation schemes in accordance with Section 4 of this Chapter;
Article 6, first paragraph, point (9)		
297	(9) relevant public bodies as well as private stakeholders by conducting targeted trainings, where appropriate in cooperation with stakeholders;	(9) relevant public bodies as well as private stakeholders by conducting targeted trainings, where appropriate in cooperation with stakeholders;
Article 6, first paragraph, point (10)		
298	(10) the NIS Cooperation Group in the exchange of best practices and information, in particular in relation to the implementation of Directive (EU) 2022/2555 pursuant to Article 14(4), point (c), of that Directive;	(10) the NIS Cooperation Group in the exchange of best practices and information, in particular in relation to the implementation of Directive (EU) 2022/2555 pursuant to Article 14(4), point (c), of that Directive;
Article 6, first paragraph, point (11)		
299	(11) the market surveillance authorities designated pursuant to Regulation (EU) 2024/2847 in their activities that aim to ensure the effective implementation of that Regulation, including support for guidance and technical advice to economic operators, support for compliance checks, evaluation of risks, joint activities and sweeps as laid down in Regulation (EU) 2024/2847;	(11) the market surveillance authorities designated pursuant to Regulation (EU) 2024/2847 in their activities that aim to ensure the effective implementation of that Regulation, including support for guidance and technical advice to economic operators, support for compliance checks, evaluation of risks, joint activities and sweeps as laid down in Regulation (EU) 2024/2847;
Article 6, first paragraph, point (12)		
300	(12) the ECCG members in the exchange of best practices and upon request from individual Member States assist national cybersecurity certification authorities in relation to the implementation of the European cybersecurity certification schemes at national level;	(12) the ECCG members in the exchange of best practices and upon request from individual Member States assist national cybersecurity certification authorities in relation to the implementation of the European cybersecurity certification schemes at national level;
Article 6, first paragraph, point (13)		
301	(13) public authorities and private stakeholders in relation to conformity assessment and evaluation activities, including conformity assessment bodies and small and medium-sized enterprises, to support a robust, competitive, inclusive and harmonised conformity assessment ecosystem supporting the implementation Regulation (EU) 2024/2847 and the European cybersecurity	(13) public authorities and private stakeholders in relation to conformity assessment and evaluation activities, including conformity assessment bodies and small and medium-sized enterprises, to support a robust, competitive, inclusive and harmonised conformity assessment ecosystem supporting the implementation Regulation (EU) 2024/2847 and the European cybersecurity

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	certification framework;	certification framework;
Article 6, first paragraph, point (14)		
302	(14) the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres established pursuant to Regulation (EU) 2021/887 by sharing information about current and emerging risks and cyber threats, including with respect to new and emerging information and communications technologies;	(14) the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres established pursuant to Regulation (EU) 2021/887 by sharing information about current and emerging risks and cyber threats, including with respect to new and emerging information and communications technologies;
Article 6, first paragraph, point (15)		
303	(15) Member States by providing technical support, including for the establishment and operation of regulatory sandboxes in the area of cybersecurity in accordance with relevant Union legislation.	(15) Member States by providing technical support, including for the establishment and operation of regulatory sandboxes in the area of cybersecurity in accordance with relevant Union legislation*, in particular Regulation (EU) 2024/2847*.
Article 7		
304	Article 7 Awareness-raising and talent pool	Article 7 Awareness-raising and talent pool
Article 7, first paragraph		
305	ENISA shall assist Member States in their efforts to raise awareness of Union policies and legislation regarding cybersecurity and promote their visibility by developing actionable tools and guidance. ENISA shall support initiatives aimed at increasing the European cybersecurity talent pool, in particular by coordinating competitions.	ENISA shall*, where appropriate in cooperation with the ECCC,* assist Member States in their efforts to raise awareness of Union policies and legislation regarding cybersecurity and promote their visibility by developing actionable tools and guidance. ENISA shall support initiatives aimed at increasing the ~~*European*~~ *Union* cybersecurity talent pool, in particular by coordinating competitions.
Article 8		
306	Article 8 Market knowledge and analyses	Article 8 Market knowledge and analyses
Article 8(1)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
307	1. ENISA shall carry out and disseminate analyses of the main market trends in the cybersecurity market on both the demand and supply sides, in particular related to the areas where European cybersecurity certification schemes exist or are planned, sectors listed in Annexes I and II to Directive (EU) 2022/2555, and product categories covered by Regulation (EU) 2024/2847, including Annexes III and IV to that Regulation.	1. ENISA shall, ***where appropriate in cooperation with the ECCC,*** carry out and disseminate analyses of the main market trends in the cybersecurity market on both the demand and supply sides, in particular related to the areas where European cybersecurity certification schemes exist or are planned, sectors listed in Annexes I and II to Directive (EU) 2022/2555, and product categories covered by Regulation (EU) 2024/2847, including Annexes III and IV to that Regulation.
Article 8(2)		
308	2. ENISA shall carry out and disseminate analyses of technological cybersecurity trends in particular in relation to activities and entities falling within the scope of Directive (EU) 2022/2555 and products with digital elements falling within the scope of Regulation (EU) 2024/2847.	2. ENISA shall carry out and disseminate analyses of technological cybersecurity trends in particular in relation to activities and entities falling within the scope of Directive (EU) 2022/2555 and products with digital elements falling within the scope of Regulation (EU) 2024/2847.
Article 8(3)		
309	3. ENISA shall build knowledge and disseminate technical advice and analyses on state-of-the-art cybersecurity tools, frameworks standards and best practices.	3. ENISA shall build knowledge and disseminate technical advice and analyses on state-of-the-art cybersecurity tools, frameworks standards and best practices.
Article 9		
310	Article 9 International cooperation	Article 9 International cooperation
Article 9, first paragraph		
311	ENISA shall contribute to the Union's efforts to cooperate with third countries and international organisations as well as within relevant international cooperation frameworks to promote international cooperation on issues related to cybersecurity, by:	ENISA shall contribute to the Union's efforts to cooperate with third countries and international organisations as well as within relevant international cooperation frameworks to promote international cooperation on issues related to cybersecurity, by:
Article 9, first paragraph, point (a)		
312	(a) where appropriate, engaging as an observer in the organisation of international exercises, and analysing and reporting to the Management Board on the outcome of such exercises;	(a) where appropriate ***and after informing the Management Board***, engaging as an observer in the organisation of international exercises, and analysing and reporting to the Management Board on the outcome of such exercises;

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 9, first paragraph, point (b)		
313	(b) at the request of the Commission, facilitating the exchange of best practices with third countries and international organisations;	(b) at the request of the Commission, facilitating the exchange of best practices with third countries and international organisations;
Article 9, first paragraph, point (c)		
314	(c) at the request of the Commission, providing it with expertise;	(c) at the request of the Commission, providing it with expertise *regarding cooperation with third countries and international organisations on issues related to cybersecurity*;
Article 9, first paragraph, point (d)		
315	(d) providing expert advice and support to the Commission on matters relating to the international recognition of European cybersecurity certificates in accordance with Article 87;	(d) providing expert advice and support to the Commission on matters relating to the international recognition of European cybersecurity certificates in accordance with Article 87;
Article 9, first paragraph, point (e)		
316	(e) providing expert advice and support to the Commission on matters concerning international standardisation and engaging with relevant international standardisation organisations, where relevant, in collaboration with the ECCG established under Article 90.	(e) providing expert advice and support to the Commission on matters concerning international standardisation and engaging with relevant international standardisation organisations, *in view of supporting Union policies related to cybersecurity, and* where relevant, in collaboration with the ECCG established under Article 90.
Article 9, first paragraph a		
316a		*The international cooperation activities carried out by ENISA under this Article shall be consistent with the international cooperation strategy adopted pursuant to Article 70.* (need to add a para 1)
Section 2		
317	Section 2 Operational Cooperation	Section 2 Operational Cooperation
Article 10		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
318	Article 10 Operational cooperation at Union level	Article 10 Operational cooperation at Union level
Article 10(1)		
319	1. ENISA shall support operational cooperation among Member States, Union entities through CERT-EU, and between other stakeholders.	1. ENISA shall support operational cooperation among Member States, Union entities through CERT-EU, and ~~between~~ ***where appropriate with*** other ***relevant*** stakeholders. Recital 24 to be further elaborated.
Article 10(2)		
320	2. ENISA shall be a member of the network of national CSIRTs established pursuant to Article 15(1) of Directive (EU) 2022/2555 and shall provide the secretariat of the CSIRTs network pursuant to Article 15(2) of Directive (EU) 2022/2555.	2. ENISA ~~*shall be a member of the network of national CSIRTs established pursuant to Article 15(1) of Directive (EU) 2022/2555 and*~~ shall provide the secretariat of the CSIRTs network ***and shall actively provide assistance for the cooperation among the CSIRTs*** pursuant to Article 15(2) of Directive (EU) 2022/2555. ***For that purpose, it shall support, advise and facilitate the activities within the network.***
Article 10(3)		
321	3. ENISA shall provide the secretariat of the European cyber crisis liaison organisation network (EU-CyCLONe) pursuant to Article 16(2), second subparagraph, of Directive (EU) 2022/2555.	3. ENISA shall provide the secretariat of the European cyber crisis liaison organisation network (EU-CyCLONe) pursuant to Article 16(2), second subparagraph, of Directive (EU) 2022/2555.
Article 10(4)		
322	4. ENISA shall support technical and operational cooperation among Member States, in particular through the CSIRTs network and EU-CyCLONe. Such support shall include:	4. ENISA shall support technical and operational cooperation among Member States, in particular through the CSIRTs network and EU-CyCLONe. Such support shall include:
Article 10(4), point (a)		
323	(a) advising on improvement of capabilities to prevent, detect, respond to and recover from incidents;	(a) ***at the request of one or more Member States,*** advising on improvement of capabilities to prevent, detect, respond to and recover from incidents;
Article 10(4), point (b)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
324	(b) at the request of one or more Member States, providing advice and assessments in relation to a specific potential or ongoing incident or cyber threat, including through the provision of expertise and facilitating the technical handling of such incidents, and through supporting the voluntary sharing of relevant information and technical solutions between Member States;	(b) at the request of one or more Member States *concerned*, providing advice and *assistance in the* assessments in relation to a specific potential or ongoing incident or cyber threat, including through the provision of expertise and facilitating the technical handling of such incidents, ~~and through~~ *including by* supporting the voluntary sharing of relevant information and technical solutions between Member States;
Article 10(4), point (c)		
325	(c) analysing vulnerabilities, threats and incidents;	(c) analysing vulnerabilities, threats and incidents;
Article 10(4), point (d)		
326	(d) at the request of one or more Member States, providing support in relation to ex post technical inquiries regarding significant incidents within the meaning of Article 23(3) of Directive (EU) 2022/2555;	(d) at the request of one or more Member States *concerned*, providing support in relation to ex post technical inquiries regarding significant incidents within the meaning of Article 23(3) of Directive (EU) 2022/2555;
Article 10(4), point (e)		
327	(e) contributing to supporting the coordinated management of large-scale cybersecurity incidents and crises at operational level, in particular by assisting EU-CyCLONe in preparing reports to political level and by facilitating timely information sharing between the CSIRTs network and EU-CyCLONe;	(e) contributing to supporting the coordinated management of large-scale cybersecurity incidents and crises at operational level, in particular by assisting EU-CyCLONe in preparing reports to political level and by facilitating timely information sharing between the CSIRTs network and EU-CyCLONe;
Article 10(4), point (ea)		
327a		*(ea) assisting in the development, exercising and revision of standard operating procedures.*
Article 10(5)		
328	5. At the request of a Member State or a Union entity in cooperation with CERT-EU, ENISA shall support consistent public communication relating to an incident or cyber threat.	5. At the request of ~~a~~ *one or more* Member ~~State~~ *States concerned,* or a Union entity in cooperation with CERT-EU, ENISA shall support *their* consistent public communication relating to an incident or cyber threat.
Article 10(6)		
329	6. ENISA shall support cooperation among Member States and through CERT-	6. ENISA shall support cooperation ~~among~~ *between Member States, between*

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	EU among Union entities with regard to the deployment of secure communications tools. ENISA shall use within the CSIRTs network and EU-CyCLONe secure communications tools which are provided by legal entities established or deemed to be established in the Union and controlled by Member States or by nationals of Member States.	Member States and ~~through CERT-EU among~~ ***Union entities, and between*** Union entities ***through CERT-EU,*** with regard to the deployment of secure communications tools***, where applicable in accordance with relevant Union law on secure communications***. ENISA shall use within the CSIRTs network and EU-CyCLONe secure communications tools which are provided by legal entities established or deemed to be established in the Union and controlled by Member States or by nationals of Member States.
Article 11		
330	Article 11 Shared cybersecurity situational awareness	Article 11 Shared cybersecurity situational awareness
Article 11(1)		
331	1. For the purposes of an enhanced shared situational awareness of the cyber threat and incident landscape among Member States and among Union entities, ENISA shall:	1. For the purposes of an enhanced shared situational awareness of the cyber threat and incident landscape ~~among Member States and among Union entities~~, ENISA shall:
Article 11(1a)		
331a		
Article 11(1a), point (a)		
332	(a) develop in cooperation with EU-CyCLONe, the CSIRTs network, the Commission, CERT-EU, Europol and other relevant Union entities, repositories of verified, reliable cyber threat intelligence, including trends in incidents, tactics, techniques and procedures;	(a) develop in cooperation with EU-CyCLONe, ***CSIRTs through*** the CSIRTs network, the Commission, CERT-EU, ***Cross-Border Cyber Hubs established pursuant to Article 5 of Regulation (EU) 2025/38,*** Europol and other relevant Union entities, ~~repositories~~***a repository*** of verified, reliable cyber threat intelligence, including trends in incidents, tactics, techniques and procedures***, and facilitate the sharing of cyber threat intelligence contained in that repository among those entities, as appropriate***;
Article 11(1a), point (b)		
333	(b) in accordance with Article 12, issue early alerts of a potential or ongoing significant or large-scale incident, or a cyber threat of a potential cross-border	(b) ~~in accordance with Article 12,~~ issue early alerts of a potential or ongoing significant or large-scale incident, or a cyber threat of a potential cross-border

	CLEAN Commission Proposal	VS.EC Council Mandate
	nature, in particular in relation to sectors listed in Annexes I and II to Directive (EU) 2022/2555;	nature, in particular in relation to sectors listed in Annexes I and II to Directive (EU) 2022/2555, *to CSIRTs and, where relevant, EU-CyCLONe*;
Article 11(1a), point (c)		
334	(c) provide timely ad hoc analyses on emerging trends in incidents upon request of the CSIRTs network, EU-CyCLONe, or the Commission;	(c) provide timely ad hoc analyses on emerging trends in incidents ~~upon request of~~*to the Member States through* the CSIRTs network, EU-CyCLONe, or the Commission*, at their request*;
Article 11(1a), point (d)		
335	(d) provide, at the request of Member States or the Commission, analysis or other information regarding an actual or perceived cybersecurity risk or threat;	(d) provide~~, at the request of Member States or the Commission~~, analysis or other information regarding an actual or perceived cybersecurity risk or threat *to Member States or the Commission, at their request*;
Article 11(1a), point (e)		
336	(e) provide analysis and technical advice regarding cybersecurity risks in products with digital elements, including to support market surveillance and by drawing up a biennial technical report on emerging trends in accordance with Article 17(3) of Regulation (EU) 2024/2847;	(e) provide analysis and technical advice regarding cybersecurity risks in products with digital elements, including to support market surveillance *authorities* and by drawing up a biennial technical report on emerging trends in accordance with Article 17(3) of Regulation (EU) 2024/2847;
Article 11(1a), point (f)		
337	(f) prepare a regular in-depth EU Cybersecurity Technical Situation Report on incidents and cyber threats, and make the report available to the Council, EU-CyCLONe, the CSIRTs network, the Commission, the European External Action Service and Europol;	(f) prepare ~~a regular~~*at least every three months an* in-depth EU Cybersecurity Technical Situation Report on incidents and cyber threats, and make the report available to the Council, EU-CyCLONe, the CSIRTs network, the Commission, the European External Action Service and Europol;
Article 11(1a), point (g)		
338	(g) monitor trends in techniques, demands and impact of ransomware attacks and provide information about such trends to the Commission, the CSIRTs network and EU-CyCLONe and Europol.	(g) monitor trends in techniques, demands and impact of ~~ransomware~~*cyber* attacks and provide information about such trends to the Commission, the CSIRTs network and EU-CyCLONe and*, where appropriate,* Europol.
Article 11(1a), point (ga)		
338a		*(ga) consolidate and analyse information about incidents, near misses, cyber*

	CLEAN Commission Proposal	VS.EC Council Mandate
		threats, risks and vulnerabilities and provide such information to Member States and the Commission.
Article 11(2)		
339	2. For the purposes of an enhanced shared situational awareness of the cyber threat and incident landscape among stakeholders, ENISA shall:	2. ~~*For the purposes of an enhanced shared situational awareness of the cyber threat and incident landscape among stakeholders, ENISA shall:*~~
Article 11(2), point (a)		
340	(a) perform analyses of cyber threats, incidents, trends, emerging technologies and their impacts, including a regular analysis addressing sectors listed in Annexes I and II to Directive (EU) 2022/2555 and relevant product categories covered by Regulation (EU) 2024/2847;	~~(a)~~*(gb)* Perform analyses of cyber threats, incidents, trends, emerging technologies and their *expected* impacts, including *aggregated indicators and* a regular analysis *and risk mapping* addressing sectors listed in Annexes I and II to Directive (EU) 2022/2555 and relevant product categories covered by Regulation (EU) 2024/2847;
Article 11(2), point (b)		
341	(b) issue, in cooperation with the Commission, and, where appropriate, the CSIRTs network, advice, guidance and best practices for the security of network and information systems, in particular for the security of the infrastructures supporting the sectors listed in Annexes I and II to Directive (EU) 2022/2555;	~~(b)~~*(gc)* issue, in cooperation with the Commission, and~~*, where appropriate,*~~ the CSIRTs network, advice, guidance and best practices for the security of network and information systems, in particular for the security of the infrastructures supporting the sectors listed in Annexes I and II to Directive (EU) 2022/2555;
Article 11(2), point (c)		
342	(c) carry out long-term strategic analyses of cyber threats and incidents in order to identify emerging trends and help prevent incidents.	~~(c)~~*(gd)* carry out long-term strategic analyses of cyber threats and incidents in order to identify emerging trends and help prevent incidents*, including on sectoral and technological trends*.
Article 11(2a)		
342a		*2a. Early alerts referred to in paragraph 1, first subparagraph, point (b), of this Regulation shall contain relevant information concerning a potential or ongoing significant or large-scale incident, or a cyber threat of a potential cross-border nature, in relation to sectors listed in Annexes I and II to Directive (EU) 2022/2555. That information may include publicly known vulnerabilities and whether they affect products with digital elements covered by Regulation (EU)*

	CLEAN Commission Proposal	VS.EC Council Mandate
		2024/2847, techniques and procedures, indicators of compromise, adversarial tactics, threat actor-specific information and recommendations on mitigation measures. Such alerts shall be issued as soon as possible.
Article 11(3)		
343	3.ENISA may make the analyses, advice, guidance, best practices and reports referred to in paragraph 2 public, in agreement with the contributing entities referred to in paragraph 2.	3.ENISA may make the analyses, advice, guidance, best practices and reports referred to in ~~paragraph 2~~ *points (gb) to (gd)* public, in agreement with the contributing entities referred to in ~~paragraph 2~~ *those points*.
Article 11(4)		
344	4.In carrying out the activities listed in paragraph 1, points (a) to (d) and (f), and paragraph 2, ENISA shall use its own analyses and, as appropriate, the information received in carrying out its tasks, including:	4.In carrying out the activities listed in paragraph 1, points (a) to (d) and ~~(f), and paragraph 2~~ *(g) to (gd)*, ENISA shall use its own analyses and, ~~as~~ *where* appropriate, the information received in carrying out its tasks, including:
Article 11(4), point (a)		
345	(a) information provided in publicly available sources, including publicly known vulnerabilities in ICT products or ICT services available in the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555;	(a) information provided in publicly available sources, including publicly known vulnerabilities in ICT products or ICT services available in the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555;
Article 11(4), point (b)		
346	(b) information shared by Member States, Union entities, CERT-EU, private sector or non-governmental partners and third country and international organisations, subject to any limitations by means of a visible marking on further distribution of that information.	(b) information shared by Member States, Union entities, CERT-EU, private sector or non-governmental partners and third ~~country~~ *countries* and international organisations~~, subject to any limitations by means of a visible marking on further distribution of that information~~. There is a general provision on information sharing protocols in Article 67 second subparagraph.
Article 11(5)		
347	5.ENISA shall cooperate closely with the Member States in the preparation of the EU Cybersecurity Technical Situation Report referred to in paragraph 1,	5.ENISA shall cooperate closely with the Member States in the preparation of the EU Cybersecurity Technical Situation Report referred to in paragraph 1,

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	point (e). The Report shall be based on publicly available information, ENISA's own analysis, and reports shared by, among others, the Member States' CSIRTs or the single points of contact established by Directive (EU) 2022/2555, both on a voluntary basis, EC3 and CERT-EU. In agreement with the contributing entities, ENISA may make an aggregated version of the Report publicly available.	point ~~(e)~~*(f)*. The Report shall be based on publicly available information, ENISA's own analysis, and reports shared by, among others, the Member States' CSIRTs or the single points of contact established by Directive (EU) 2022/2555, both on a voluntary basis, EC3 and CERT-EU. ~~In~~ *ENISA shall make the report available to the Council, EU-CyCLONe, the CSIRTs network, the Commission, the European External Action Service and Europol. Subject to the* agreement ~~with~~ *of* the contributing entities, ENISA may make an aggregated version of the Report publicly available. MSs suggestion "ENISA shall encourage Member States to share information needed for the report to reflect the situation in all Member States." to be reflected in a new recital.
Article 12		
348	Article 12 Early alerts	Article 12 ~~*Early alerts*~~
Article 12(1)		
349	1. Early alerts referred to in Article 11(1), first subparagraph, point (b), of this Regulation shall contain relevant information concerning a potential or ongoing significant or large-scale incident, or a cyber threat of a potential cross-border nature, in relation to sectors listed in Annexes I and II to Directive (EU) 2022/2555. Such information may include publicly known vulnerabilities and whether they affect products with digital elements covered by Regulation (EU) 2024/2847, techniques and procedures, indicators of compromise, adversarial tactics, threat actor-specific information and recommendations on mitigation measures.	1. ~~*Early alerts referred to in Article 11(1), first subparagraph, point (b), of this Regulation shall contain relevant information concerning a potential or ongoing significant or large-scale incident, or a cyber threat of a potential cross-border nature, in relation to sectors listed in Annexes I and II to Directive (EU) 2022/2555. Such information may include publicly known vulnerabilities and whether they affect products with digital elements covered by Regulation (EU) 2024/2847, techniques and procedures, indicators of compromise, adversarial tactics, threat actor-specific information and recommendations on mitigation measures.*~~
Article 12(2)		
350	2. Early alerts referred to in Article 11(1), first subparagraph, point (b), shall be issued as soon as possible to the CSIRT or CSIRTs concerned, and, where appropriate, to the CSIRTs network and EU-CyCLONe.	2. ~~*Early alerts referred to in Article 11(1), first subparagraph, point (b), shall be issued as soon as possible to the CSIRT or CSIRTs concerned, and, where appropriate, to the CSIRTs network and EU-CyCLONe.*~~

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 12(3)		
351	3. ENISA shall offer an early alert service to entities operating in sectors listed in Annexes I and II to Directive (EU) 2022/2555.	3. ~~*ENISA shall offer an early alert service to entities operating in sectors listed in Annexes I and II to Directive (EU) 2022/2555.*~~
Article 12(4)		
352	4. The service referred to in paragraph 3 shall be provided upon a request of the entity and in a machine-readable format made publicly available. That service shall include sharing of information on cyber threat indicators and recommendations on mitigation measures.	4. ~~*The service referred to in paragraph 3 shall be provided upon a request of the entity and in a machine-readable format made publicly available. That service shall include sharing of information on cyber threat indicators and recommendations on mitigation measures.*~~
Article 12(5)		
353	5. ENISA shall establish a procedure to disseminate the early alerts to entities referred to in paragraph 3.	5. ~~*ENISA shall establish a procedure to disseminate the early alerts to entities referred to in paragraph 3.*~~
Article 13		
354	Article 13 Support in incident response and review	Article 13 Support in incident response and review
Article 13(1)		
355	1. ENISA shall operate and administer the EU Cybersecurity Reserve, in full or in part, in accordance with Regulation (EU) 2025/38.	1. ENISA shall operate and administer the EU Cybersecurity Reserve, in full or in part, in accordance with Regulation (EU) 2025/38.
Article 13(2)		
356	2. At the request of the Commission or EU-CyCLONe, ENISA, with the support of the CSIRTs network and with the approval of the Member State concerned, shall review and assess significant cybersecurity incidents or large-scale cybersecurity incidents in accordance with Article 21 of Regulation (EU) 2025/38.	2. At the request of the Commission or EU-CyCLONe, ENISA, with the support of the CSIRTs network and with the approval of the Member State concerned, shall review and assess significant cybersecurity incidents or large-scale cybersecurity incidents in accordance with Article 21 of Regulation (EU) 2025/38.
Article 13(3)		
357	3. ENISA shall assist, in cooperation with Europol and CSIRTs or other competent authorities as applicable, individual essential and important entities	3. ENISA shall assist, in cooperation with Europol and CSIRTs or other competent authorities, as applicable, individual essential and important entities

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	listed in Annexes I and II to Directive (EU) 2022/2555 in preparing, responding to and recovering from a ransomware incident. For that purpose, ENISA shall establish a helpdesk and in particular make use of the enhanced shared situational awareness of the cyber threat and incident landscape pursuant to Article 11(1), first subparagraph, points (a) and (g) of this Regulation.	listed in Annexes I and II to Directive (EU) 2022/2555 in preparing *for*, responding to and recovering from ~~*a ransomware incident*~~*incidents*. For that purpose, ENISA shall ~~*establish a helpdesk and in particular*~~ make use of the enhanced shared situational awareness of the cyber threat and incident landscape pursuant to Article 11(1), first subparagraph, points (a) and (g) of this Regulation.
Article 14		
358	Article 14 Cybersecurity exercises at Union level	Article 14 Cybersecurity exercises at Union level
Article 14(1)		
359	1. ENISA shall support the Commission in compiling an annual rolling programme of Union-level cybersecurity exercises	1. ENISA shall support the Commission in compiling an annual rolling programme of Union-level cybersecurity exercises To add to Recital 38 The rolling programme of cybersecurity exercises should be prepared in cooperation with the Member States and shall take into account of exercises of the Union Civil Protection Mechanism (UCPM) and other Union-level crisis response mechanisms exercises, including exercises outlined in the EU Blueprint for Cyber Crisis Management and in the EU Critical Infrastructure Blueprint.
Article 14(2)		
360	2. ENISA shall maintain a repository of lessons learned from the exercises referred to in paragraph 1 and recommend to Member States and, where relevant, to Union entities how to implement the lessons learned effectively and efficiently.	2. ENISA*, in its role of secretariat of the CSIRTs network and EU-CyCLONe,* shall maintain a repository of lessons learned from the exercises referred to in paragraph 1 and recommend to Member States and, where relevant, to Union entities how to implement the lessons learned effectively and efficiently.
Article 14(3)		
361	3. At the request of EU-CyCLONe, the Commission, ENISA shall organise, or contribute to the organisation of, cybersecurity exercises at Union level, including testing preparedness to respond to large-scale cybersecurity incidents	3. At the request of EU-CyCLONe, the Commission *or the CSIRTs network*, ENISA shall *regularly* organise, or contribute to the organisation of, cybersecurity exercises at Union level, including testing preparedness to respond

	CLEAN Commission Proposal	VS.EC Council Mandate
	and crises at Union level.	to large-scale cybersecurity incidents and crises at Union level. *ENISA shall, for that purpose, closely cooperate with EU-CyCLONe, CSIRTs Network, and the Commission, as applicable.*
Article 14(4)		
362	4. At the request of Member States, ENISA shall support them in organising national cybersecurity exercises.	4. At the request of Member States, ENISA shall support them in organising national cybersecurity exercises *and facilitate the exchange of best practices from national exercises on large-scale cybersecurity incidents and crises*. Recital to be incorporated regarding ENISA providing strategic and technical guidance.
Article 14(5)		
363	5. At the request of CERT-EU, ENISA shall contribute to the organisation of cybersecurity exercises organised by CERT-EU pursuant to Article 13(7) of Regulation (EU, Euratom) 2023/2841.	5. At the request of CERT-EU, ENISA shall contribute to the organisation of cybersecurity exercises organised by CERT-EU pursuant to Article 13(7) of Regulation (EU, Euratom) 2023/2841.
Article 15		
364	Article 15 Provision of tools and platforms	Article 15 Provision of tools and platforms
Article 15(1)		
365	1. ENISA shall establish, provide, operate, maintain and update as necessary, operational technical tools, including platforms related to cybersecurity at Union level, in particular the single reporting platform established pursuant to Article 16(1) of Regulation (EU) 2024/2847 [and the single-entry point for incident reporting established pursuant to Article 23a of Directive (EU) 2022/2555], and testing tools to support the implementation of conformity assessment procedures in accordance with the relevant Union legislation.	1. ENISA shall establish, provide, operate, maintain and update as necessary, operational technical tools, including platforms related to cybersecurity at Union level, in particular the single reporting platform established pursuant to Article 16(1) of Regulation (EU) 2024/2847 [and the single-entry point for incident reporting established pursuant to Article 23a of Directive (EU) 2022/2555]~~, *and testing tools to support the implementation of conformity assessment procedures in accordance with the relevant Union legislation*~~. SEP to be left in brackets.
Article 15(1a)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
365a		*1a. Subject to approval of the Management Board, ENISA shall develop, provide, operate, maintain, and update as necessary testing tools to support the implementation of conformity assessment procedures in accordance with the relevant Union legislation.*
Article 15(2)		
366	2. Where appropriate for the purposes of paragraph 1, ENISA shall cooperate and exchange information with the CSIRTs network and, where applicable, market surveillance authorities.	2. Where appropriate for the purposes of paragraph 1, ENISA shall cooperate and exchange information with the CSIRTs network and, where applicable, market surveillance authorities.
Article 16		
367	Article 16 Vulnerability management services	Article 16 Vulnerability management services
Article 16, first paragraph		
368	ENISA shall develop a common Union vulnerability management service capacity and provide vulnerability management services to stakeholders by:	ENISA shall develop a common Union vulnerability management service capacity ~~*and provide vulnerability management services to stakeholders by:*~~ *by*
Article 16, first paragraph, point (a)		
369	(a) maintaining the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555;	(a) maintaining the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555;
Article 16, first paragraph, point (b)		
370	(b) providing vulnerability management services to stakeholders, building on the European vulnerability database and making use of relevant information available to ENISA;	(b) providing vulnerability management services to stakeholders, building on the European vulnerability database ~~*and making use of relevant information available to ENISA.*~~*;*
Article 16, first paragraph, point (ba)		
370a		*(ba) where appropriate, making use of relevant information available to ENISA, to provide advisories, corrective or mitigating measures or detection mechanisms related to vulnerabilities;*
Article 16, first paragraph, point (c)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
371	(c) where appropriate, entering into structured cooperation with organisations providing programmes, registries or databases similar to the European vulnerability database;	(c) where appropriate, entering into structured cooperation with organisations providing programmes, registries or databases similar to the European vulnerability database;
Article 16, first paragraph, point (d)		
372	(d) actively supporting the CSIRTs designated as coordinators pursuant to Article 12(1) of Directive (EU) 2022/2555 with regard to the management of the coordinated disclosure of vulnerabilities which may have a significant impact on entities in more than one Member State;	(d) actively supporting the CSIRTs designated as coordinators pursuant to Article 12(1) of Directive (EU) 2022/2555 with regard to the management of the coordinated disclosure of vulnerabilities which may have a significant impact on entities in more than one Member State;
Article 16, first paragraph, point (da)		
372a		*(da)supporting Member States, upon request and where appropriate, in the timely identification of entities potentially affected by a known vulnerability, in the targeted notification of such entities, and in the facilitation of coordinated remediation, including by supporting the development and dissemination of practical mitigation and patching guidance, while respecting the responsibilities of CSIRTs and CERT-EU."*
Article 16, first paragraph, point (e)		
373	(e) developing and maintaining methodologies and governance mechanisms for vulnerability identification and coordinated disclosure, in cooperation with national competent authorities, CSIRTs, industry and the research community.	(e) Developing ~~and~~, maintaining *and promoting* methodologies and governance mechanisms for vulnerability identification and coordinated disclosure, in cooperation with national competent authorities, CSIRTs, industry and the research community. MSs suggestion regarding specifying the scope, processes, and minimum service components of the vulnerability management services referred to in point (b) to considered in Recital 39.
Section 3		
374	Section 3 Cybersecurity Certification and Standardisation	Section 3 Cybersecurity Certification and Standardisation
Article 17		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
375	Article 17 Cybersecurity certification	Article 17 Cybersecurity certification
Article 17(1)		
376	1.ENISA shall contribute to and promote the development and implementation of Union policy on cybersecurity certification as established in Title III of this Regulation. ENISA shall be in charge of:	1.ENISA shall contribute to and promote the development and implementation of Union policy on cybersecurity certification as established in Title III of this Regulation. ENISA shall be ~~*in charge of*~~ ***responsible for***.
Article 17(1), point (a)		
377	(a) preparing candidate European cybersecurity certification schemes ('candidate schemes') for ICT products, ICT services, ICT processes, managed security services and the cyber posture of entities in accordance with Article 74 and, where applicable, developing technical specifications in accordance with Article 77;	(a) preparing candidate European cybersecurity certification schemes ('candidate schemes') for ICT products, ICT services, ICT processes, managed security services and the cyber posture of entities in accordance with Article 74 and, where applicable, developing technical specifications in accordance with Article 77;
Article 17(1), point (b)		
378	(b) maintaining adopted European cybersecurity certification schemes in accordance with Article 75, including in view of a possible review of the adopted European cybersecurity certification schemes in accordance with Article 76;	(b) maintaining adopted European cybersecurity certification schemes in accordance with Article 75, including in view of a possible review of the adopted European cybersecurity certification schemes in accordance with Article 76;
Article 17(1), point (c)		
379	(c) promoting the uptake of adopted schemes and maintaining a dedicated website providing information on, and publicising, European cybersecurity certification schemes, European cybersecurity certificates and EU statements of conformity in accordance with Article 79;	(c) promoting the uptake of adopted schemes and maintaining a dedicated website providing information on, and publicising, European cybersecurity certification schemes, European cybersecurity certificates and EU statements of conformity in accordance with Article 79;
Article 17(1), point (d)		
380	(d) organising capacity-building related to certification processes, evaluation activities, peer review and peer assessment, including by providing support to Member States at their request in accordance with Article 6, point (12).	(d) organising capacity-building related to certification ~~*processes,*~~***and*** evaluation activities, peer review and peer assessment, including by providing support to Member States at their request in accordance with Article 6, point (12).
Article 17(2)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
381	2. ENISA shall support the Commission in the following activities:	2. ENISA shall support the Commission in the following activities:
Article 17(2), point (a)		
382	(a) the governance of the ECCG pursuant to Article 90;	(a) the governance of the ECCG pursuant to Article 90;
Article 17(2), point (b)		
383	(b) organising a European Cybersecurity Certification Assembly in accordance with Article 72(1);	(b) organising a European Cybersecurity Certification Assembly in accordance with Article 72(1);
Article 17(2), point (c)		
384	(c) relating to the international recognition of European cybersecurity certificates in accordance with Article 87;	(c) ***activities*** relating to ***the process of*** the international recognition of European cybersecurity certificates in accordance with Article 87;
Article 17(2), point (d)		
385	(d) organising peer reviews pursuant to Article 89;	(d) organising peer reviews pursuant to Article 89;
Article 17(2), point (e)		
386	(e) preparing model provisions to be referenced in the European cybersecurity certification schemes for ICT products, ICT services, ICT processes, managed security services and cyber posture of entities in accordance with Article 81(5).	(e) preparing model provisions to be referenced in the European cybersecurity certification schemes for ICT products, ICT services, ICT processes, managed security services and cyber posture of entities in accordance with Article 81(5).
Article 18		
387	Article 18 Standardisation, technical specifications and guidance	Article 18 Standardisation, technical specifications and guidance
Article 18(1)		
388	1. ENISA shall draft technical specifications and guidance to support the implementation of Union legislation in the field of cybersecurity. When drafting those technical specifications, ENISA shall consider existing European and international standards as well as other relevant technical specifications. ENISA shall ensure the consistency of its technical specifications and guidance.	1. ENISA shall draft technical specifications and guidance***, in consultation with Member States and other relevant stakeholders,*** to support the implementation of Union legislation in the field of cybersecurity. When drafting those technical specifications, ENISA shall consider existing European ~~and~~ , international ***or national*** standards as well as other relevant technical specifications. ENISA shall ensure the consistency of its technical specifications and guidance.

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 18(2)		
389	2.ENISA shall monitor and, where relevant, participate and lead in standardisation development activities at Union level and, in accordance with Article 9, at international level, in view of supporting Union policies related to cybersecurity.	2.ENISA shall monitor and, where relevant, participate ~~*and lead*~~ in standardisation development activities at Union level and, in accordance with Article 9, at international level, in view of supporting Union policies related to cybersecurity. Recital 41 to be amended "by participating in the activities of European standardisation organisations and of international standardisation organisations, including, as appropriate, through drafting contributions, steering or facilitating the technical development of standards."
Article 18(3)		
390	3.ENISA shall support the development and evaluation of cryptographic algorithms. Where a cryptographic algorithm is evaluated positively by ENISA, ENISA shall cooperate, in accordance with Regulation (EU) No 1025/2012, with the European standardisation bodies to support its standardisation.	3.ENISA shall support the development ~~*and*~~ *,* evaluation *processes and update* of cryptographic algorithms. Where a cryptographic algorithm is evaluated positively *in the evaluation processes supported or coordinated* by ENISA, ENISA shall cooperate, in accordance with Regulation (EU) No 1025/2012, with the European standardisation bodies to support its standardisation.
Article 18(4)		
391	4.ENISA shall provide technical advice to the Commission and, where relevant, the Member States, on appropriate standards or technical specifications in support of Union policies related to cybersecurity, including for Union harmonisation legislation in the field of cybersecurity, in particular Regulation (EU) 2024/2847, technical areas for the purpose of Article 25 of Directive (EU) 2022/2555, and European cybersecurity certification schemes pursuant to Article 81(1), point (d).	4.ENISA shall provide technical advice to the Commission and, where relevant, the Member States, on appropriate standards or technical specifications in support of Union policies related to cybersecurity, including for Union harmonisation legislation in the field of cybersecurity, in particular Regulation (EU) 2024/2847, technical areas for the purpose of Article 25 of Directive (EU) 2022/2555, and European cybersecurity certification schemes pursuant to Article 81(1), point (d).
Article 18(5)		
392	5.ENISA shall assist the Commission in the assessment of draft harmonised standards to support the implementation of Union harmonisation legislation in the field of cybersecurity.	5.ENISA shall assist the Commission in the assessment of draft harmonised standards to support the implementation of Union harmonisation legislation in the field of cybersecurity.

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 18(6)		
393	6.ENISA shall promote the uptake of European and international standards for cybersecurity.	6.ENISA shall promote the uptake of European and international standards for cybersecurity.
Article 18(7)		
394	7.ENISA shall carry out the tasks referred to in paragraphs 1 to 6 with integrity, impartiality and confidentiality, including by withdrawing or pausing its participation from specific technical bodies when such a participation conflicts with other tasks or objectives.	7.ENISA shall carry out the tasks referred to in paragraphs 1 to 6 with integrity, impartiality, ***transparency*** and confidentiality, including by withdrawing or pausing its participation from specific technical bodies when such a participation conflicts with other tasks or objectives.
Section 4		
395	Section 4 Implementation of the Cybersecurity Skills Academy	Section 4 Implementation of the Cybersecurity Skills Academy
Article 19		
396	Article 19 European Cybersecurity Skills Framework	Article 19 European Cybersecurity Skills Framework
Article 19(1)		
397	1.ENISA shall develop and make publicly available a European Cybersecurity Skills framework ('ECSF'). Before making the ECSF publicly available or updating it pursuant to paragraph 4, ENISA shall consult the Commission.	1.ENISA shall develop and make publicly available a European Cybersecurity Skills framework ('ECSF'). Before making the ECSF publicly available or updating it pursuant to paragraph 4, ENISA shall consult the Commission ***and Member States***.
Article 19(2)		
398	2.The ECSF shall define profiles of cybersecurity professionals and association of specific tasks, skills and knowledge to a given role profile. The use of the ECSF shall be voluntary for public and private entities.	2.The ECSF shall define profiles of cybersecurity professionals and association of specific tasks, skills and knowledge to a given role profile. The use of the ECSF shall be voluntary for public and private entities.
Article 19(3)		
399	3.ENISA may consult stakeholders in the development and uptake of the ECSF.	3.***"***ENISA ~~*may*~~ ***shall*** consult ***private and public*** stakeholders in the development and uptake of the ECSF.***"***
Article 19(4)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
400	4. ENISA shall assess the need to update the ECSF on a regular basis and, where relevant, update it.	4. ENISA shall assess the need to update the ECSF on a regular basis and, where relevant, update it.
Article 20		
401	Article 20 Development, adoption and maintenance of European individual cybersecurity skills attestation schemes	Article 20 Development, adoption and maintenance of European individual cybersecurity skills attestation schemes
Article 20(1)		
402	1. ENISA shall develop, adopt and maintain European individual cybersecurity skills attestation schemes. The use of European individual cybersecurity skills attestation schemes shall be voluntary for national public bodies and private entities, unless otherwise specified by national law.	1. ENISA shall develop, adopt and maintain European individual cybersecurity skills attestation schemes. The use of European individual cybersecurity skills attestation schemes shall be voluntary for national public bodies and private entities, unless otherwise specified by national law.
Article 20(2)		
403	2. Prior to initiating a new European individual cybersecurity skills attestation scheme, ENISA shall consult the Commission. ENISA shall only adopt such a scheme following a positive opinion from the Commission. When preparing a European individual cybersecurity skills attestation scheme, ENISA may consult relevant stakeholders.	2. Prior to initiating a new European individual cybersecurity skills attestation scheme, ENISA shall consult the Commission *and Member States*. ENISA shall only adopt such a scheme following a positive opinion from the Commission. When preparing a European individual cybersecurity skills attestation scheme, ENISA ~~may~~ *shall* consult relevant stakeholders *including the European Cybersecurity Industrial, Technology and Research Competence Centre*. Recital 48 to be amended accordingly.
Article 20(3)		
404	3. A European individual cybersecurity skills attestation scheme shall include the following:	3. A European individual cybersecurity skills attestation scheme shall include the following:
Article 20(3), point (a)		
405	(a) subject matter and scope of the attestation scheme based on ECSF role profiles or subsets thereof;	(a) subject matter and scope of the attestation scheme based on ECSF role profiles or subsets thereof;
Article 20(3), point (b)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
406	(b) requirements applicable to individuals trained to perform assessments ('assessors') in accordance with Article 21, the necessary skills, knowledge and experience as well as training methods;	(b) requirements applicable to individuals trained to perform assessments ('assessors') in accordance with Article 21, the necessary skills, knowledge and experience as well as training methods;
Article 20(3), point (c)		
407	(c) market uptake analysis specific to each attestation scheme;	(c) market uptake analysis specific to each attestation scheme;
Article 20(3), point (d)		
408	(d) the learning outcomes, assessment methods, and conditions that authorised attestation providers shall use to evaluate an individual's demonstration of the required skills in accordance with Article 21;	(d) the learning outcomes, assessment methods, and conditions that authorised attestation providers shall use to evaluate an individual's demonstration of the required skills in accordance with Article 21;
Article 20(3), point (e)		
409	(e) where relevant, one or more proficiency levels;	(e) where relevant, one or more proficiency levels;
Article 20(3), point (f)		
410	(f) rules concerning the retention of records by authorised attestation providers;	(f) rules concerning the retention of records by authorised attestation providers;
Article 20(3), point (g)		
411	(g) the content and the format of the European individual cybersecurity skills attestations, taking into due consideration Article 21(5), point (e);	(g) the content and the format of the European individual cybersecurity skills attestations, taking into due consideration Article 21(5), point (e);
Article 20(3), point (h)		
412	(h) maximum period of validity of a European individual cybersecurity skills attestation issued under the attestation scheme.	(h) maximum period of validity of a European individual cybersecurity skills attestation issued under the attestation scheme~~.~~*;*
Article 20(3), point (ha)		
412a		*(ha) conditions for the renewal of a European individual cybersecurity skills attestation;*
Article 20(3), point (hb)		
412b		*(hb) conditions under which alternative qualifications, including certification*

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
		and attestations, already demonstrate acquired skills and learning outcomes, including with regards to proficiency levels, and their effects on the assessments.
Article 20(4)		
413	4. A European individual cybersecurity skills attestation scheme may include the indicative cost of a European individual cybersecurity skills attestation.	4. A European individual cybersecurity skills attestation scheme may include the indicative cost of a European individual cybersecurity skills attestation. *When determining and publishing such indicative costs, ENISA shall ensure that the attestation schemes remain financially accessible, proportionate and do not create undue barriers to participation, in particular for individuals and small and medium-sized enterprises.* See also Art. 23 (d) on ENISA's website listing the indicative costs.
Article 20(5)		
414	5. ENISA shall ensure close cooperation with Member States throughout preparation of the European individual cybersecurity skills attestation schemes.	5. ENISA shall ensure close cooperation with Member States throughout preparation of the European individual cybersecurity skills attestation schemes.
Article 20(6)		
415	6. The modification of a European individual cybersecurity skills attestation scheme shall not affect the authorisation granted pursuant to Article 22(3)(a), which shall remain valid for the period it is granted for.	6. The modification of a European individual cybersecurity skills attestation scheme shall not affect the authorisation granted pursuant to Article 22(3)(a), which shall remain valid for the period it is granted for.
Article 21		
416	Article 21 Authorised attestation providers	Article 21 Authorised attestation providers
Article 21(1)		
417	1. Authorised attestation providers shall assess whether individuals meet the requirements of a European individual cybersecurity skills attestation scheme and, where those requirements are met, issue European individual cybersecurity skills attestations. Attestation providers may hold several authorisations, each granted for one European individual cybersecurity skills attestation scheme.	1. Authorised attestation providers shall assess whether individuals meet the requirements of a European individual cybersecurity skills attestation scheme and, where those requirements are met, issue European individual cybersecurity skills attestations. Attestation providers may hold several authorisations, each granted for one European individual cybersecurity skills attestation scheme.

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 21(2)		
418	2. ENISA shall provide guidance to and conduct obligatory training of assessors regarding the requirements and assessment methods included in the European individual cybersecurity skills attestation scheme as referred to in Article 20(3), point (b).	2. ENISA shall provide guidance to and conduct obligatory training of assessors regarding the requirements and assessment methods included in the European individual cybersecurity skills attestation scheme as referred to in Article 20(3), point (b).
Article 21(3), first subparagraph		
419	3. Entities wishing to become authorised attestation providers or renew their authorisation ('applicants') shall submit an application to ENISA. They shall meet the following requirements:	3. Entities wishing to become authorised attestation providers or renew their authorisation ('applicants') shall submit an application to ENISA. They shall meet the following requirements:
Article 21(3), first subparagraph, point (a)		
420	(a) they shall have legal personality;	(a) they shall have legal personality;
Article 21(3), first subparagraph, point (b)		
421	(b) they shall be capable of carrying out the tasks laid down in this Regulation in relation to European individual cybersecurity skills attestations, regardless of whether the assessment is carried out by the authorised attestation provider itself or on its behalf and under its responsibility;	(b) they shall be capable of carrying out the tasks laid down in this Regulation in relation to European individual cybersecurity skills attestations, regardless of whether the assessment is carried out by the authorised attestation provider itself or on its behalf and under its responsibility;
Article 21(3), first subparagraph, point (c)		
422	(c) they shall have the means necessary to perform the technical and administrative tasks connected with the European individual cybersecurity skills attestation scheme in an appropriate manner and have access to all necessary equipment and facilities.	(c) they shall have the means necessary to perform the technical and administrative tasks connected with the European individual cybersecurity skills attestation scheme in an appropriate manner and have access to all necessary equipment and facilities.
Article 21(3), second subparagraph		
423	For the purposes of the first subparagraph, point (b), any subcontracting to, or consultation of, external staff shall be properly documented, shall not involve any intermediaries and shall be subject to a written agreement covering, among other things, confidentiality and conflicts of interest.	For the purposes of the first subparagraph, point (b), any subcontracting to, or consultation of, external staff shall be properly documented, shall not involve any intermediaries and shall be subject to a written agreement covering, among other things, confidentiality and conflicts of interest.

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 21(4)		
424	4. Applicants shall not be high-risk suppliers.	4. Applicants *and authorised attestation providers* shall not be high-risk suppliers. *"*
Article 21(5)		
425	5. Authorised attestation providers shall meet the following obligations:	5. Authorised attestation providers shall meet the following obligations:
Article 21(5), point (a)		
426	(a) for the implementation of each European individual cybersecurity skills attestation scheme:	(a) for the implementation of each European individual cybersecurity skills attestation scheme:
Article 21(5), point (a)(i)		
427	(i) have at their disposal the necessary assessors and personnel to carry out their activities as established in that scheme in a timely manner;	(i) have at their disposal the necessary assessors and personnel to carry out their activities as established in that scheme in a timely manner;
Article 21(5), point (a)(ii)		
428	(ii) ensure that assessors observe professional secrecy, are impartial and perform their work independently and with the highest degree of professional integrity;	(ii) ensure that assessors observe professional secrecy, are impartial and perform their work independently and with the highest degree of professional integrity;
Article 21(5), point (a)(iii)		
429	(iii) have written procedures for carrying out their activities under the scheme that they are authorised for.	(iii) have written procedures for carrying out their activities under the scheme that they are authorised for.
Article 21(5), point (b)		
430	(b) not assess or issue European individual cybersecurity skills attestations to their own assessors;	(b) not assess or issue European individual cybersecurity skills attestations to their own assessors;
Article 21(5), point (c)		
431	(c) ensure, where relevant by putting in place appropriate safeguards, that their assessors can perform their work independently, in particular where such individuals belong to their own structure or are employees or learners of such a structure;	(c) ensure, where relevant by putting in place appropriate safeguards, that their assessors can perform their work independently, in particular where such individuals belong to their own structure or are employees or learners of such a structure;

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 21(5), point (d)		
432	(d) not engage in any activity that may conflict with the independence of judgement or integrity of their assessors;	(d) not engage in any activity that may conflict with the independence of judgement or integrity of their assessors;
Article 21(5), point (e)		
433	(e) ensure that, at the request of the individual, electronic attestations of European individual cybersecurity skills attestations are issued as electronic attestations of attributes in a format that can be stored in the European Digital Identity Wallets set out in Regulation (EU) No 910/2014.	(e) ensure that, at the request of the individual, electronic attestations of European individual cybersecurity skills attestations are issued as electronic attestations of attributes in a format that can be stored in the European Digital Identity Wallets set out in Regulation (EU) No 910/2014.
Article 21(6)		
434	6. Authorised attestation providers shall immediately inform ENISA if any of the requirements listed in paragraphs 3 and 4 or the obligations listed in paragraph 5, are no longer met or if any doubt that those requirements or obligations are not met, arises, including regarding the independence of assessors.	6. Authorised attestation providers shall immediately inform ENISA if any of the requirements listed in paragraphs 3 and 4 or the obligations listed in paragraph 5, are no longer met or if any doubt that those requirements or obligations are not met, arises, including regarding the independence of assessors.
Article 21(7)		
435	7. Authorised attestation providers may request a fee from individuals for assessing and issuing the European individual cybersecurity skills attestations, taking into account the indicative cost of a European individual cybersecurity skills attestation pursuant to Article 20(4) and made public on a dedicated website in accordance with Article 23, point (d).	7. Authorised attestation providers may request a fee from individuals for assessing and issuing the European individual cybersecurity skills attestations, taking into account the indicative cost of a European individual cybersecurity skills attestation pursuant to Article 20(4) and made public on a dedicated website in accordance with Article 23, point (d).
Article 21(8)		
436	8. Applicants and authorised attestation providers shall allow ENISA to conduct evaluations as part of the application process or maintenance of the authorisation and share all relevant information to ensure the requirements laid down in paragraphs 3 and 4, or the obligations laid down in paragraph 5, are met or continue to be met in accordance with Article 22(2).	8. Applicants and authorised attestation providers shall allow ENISA to conduct evaluations as part of the application process or maintenance of the authorisation and share all relevant information to ensure the requirements laid down in paragraphs 3 and 4, or the obligations laid down in paragraph 5, are met or continue to be met in accordance with Article 22(2).
Article 22		
437	Article 22	Article 22

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	Examination of applications to become an authorised attestation provider and maintenance of authorisations	Examination of applications to become an authorised attestation provider and maintenance of authorisations
Article 22(1)		
438	1. Applicants shall pay a fee to ENISA for the examination of their application. Authorised attestation providers shall pay a fee to ENISA for the maintenance of their authorisation.	1. Applicants shall pay a fee to ENISA for the examination of their application. Authorised attestation providers shall pay a fee to ENISA for the maintenance of their authorisation.
Article 22(2)		
439	2. ENISA shall evaluate whether the requirements laid down in Article 21(3) and (4) and the obligations laid down in Article 21(5) are met or continue to be met by applicants and authorised attestation providers.	2. ENISA shall evaluate whether the requirements laid down in Article 21(3) and (4) and the obligations laid down in Article 21(5) are met or continue to be met by applicants and authorised attestation providers.
Article 22(3), first subparagraph		
440	3. After examining an application against the requirements laid down in Article 21(3) and (4), ENISA may issue one of the following decisions:	3. After examining an application against the requirements laid down in Article 21(3) and (4), ENISA may issue one of the following decisions:
Article 22(3), first subparagraph, point (a)		
441	(a) granting the applicant the status of authorised attestation provider or renewing it;	(a) granting the applicant the status of authorised attestation provider or renewing it;
Article 22(3), first subparagraph, point (b)		
442	(b) rejecting the application to become an authorised attestation provider or not renewing it;	(b) rejecting the application to become an authorised attestation provider or not renewing it;
Article 22(3), first subparagraph, point (c)		
443	(c) closing the processing of the application due to the applicant's inaction following a request for additional information by ENISA.	(c) closing the processing of the application due to the applicant's inaction following a request for additional information by ENISA.
Article 22(3), second subparagraph		
444	ENISA may amend, suspend or revoke such decisions based on its evaluation pursuant to Article 22(2) or in the case referred to in Article 21(6).	ENISA may amend, suspend or revoke such decisions based on its evaluation pursuant to Article 22(2) or in the case referred to in Article 21(6).

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 22(4)		
445	4. ENISA shall issue the decision referred to in paragraph 3 within three months from the date of submission of an application in accordance with Article 21(3). Where ENISA requested the applicant for the additional information, ENISA shall issue the decision referred to in paragraph 3 within one month of receiving additional information.	4. ENISA shall issue the decision referred to in paragraph 3 within three months from the date of submission of an application in accordance with Article 21(3). Where ENISA requested the applicant for the additional information, ENISA shall issue the decision referred to in paragraph 3 within one month of receiving additional information.
Article 22(5)		
446	5. The decision referred to in paragraph 3, point (a) shall have a maximum duration of three years and indicate the fee related to the yearly maintenance of the authorisation.	5. The decision referred to in paragraph 3, point (a) shall have a maximum duration of three years and indicate the fee related to the yearly maintenance of the authorisation.
Article 22(6)		
447	6. ENISA shall ensure that its activities relating to the development and adoption of European individual cybersecurity skills attestation schemes as laid down in Article 20 are strictly separated and carried out independently from the activities on the examination of applications and on evaluations set out in paragraphs 2 and 3 of this Article.	6. ENISA shall ensure that its activities relating to the development and adoption of European individual cybersecurity skills attestation schemes as laid down in Article 20 are strictly separated and carried out independently from the activities on the examination of applications and on evaluations set out in paragraphs 2 and 3 of this Article.
Article 23		
448	Article 23 Public information	Article 23 Public information
Article 23, first paragraph		
449	ENISA shall maintain and regularly update a dedicated website providing public information on:	ENISA shall maintain and regularly update a dedicated website providing public information on:
Article 23, first paragraph, point (a)		
450	(a) the ECSF, including the framework and its timeline for update;	(a) the ECSF, including the framework and its timeline for update;
Article 23, first paragraph, point (b)		
451	(b) the European individual cybersecurity skills attestation schemes, their	(b) the European individual cybersecurity skills attestation schemes, their

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	progress and timelines for their development;	progress and timelines for their development;
Article 23, first paragraph, point (c)		
452	(c) the fees associated with each European individual cybersecurity skills attestation scheme adopted pursuant to Article 47 of this Regulation;	(c) the fees associated with each European individual cybersecurity skills attestation scheme adopted pursuant to Article 47 of this Regulation;
Article 23, first paragraph, point (d)		
453	(d) the indicative cost of a European individual cybersecurity skills attestation in accordance with Article 20(4);	(d) the indicative cost of a European individual cybersecurity skills attestation in accordance with Article 20(4);
Article 23, first paragraph, point (e)		
454	(e) the list of authorised attestation providers.	(e) the list of authorised attestation providers.
Chapter III		
455	Chapter III Organisation of ENISA	Chapter III Organisation of ENISA
Article 24		
456	Article 24 Administrative and management structure of ENISA	Article 24 Administrative and management structure of ENISA
Article 24, first paragraph		
457	The administrative and management structure of ENISA shall comprise:	The administrative and management structure of ENISA shall comprise:
Article 24, first paragraph, point (a)		
458	(a) a Management Board which shall exercise the functions set out in Article 28;	(a) a Management Board which shall exercise the functions set out in Article 28;
Article 24, first paragraph, point (b)		
459	(b) an Executive Board which shall exercise the functions set out in Article 30;	(b) an Executive Board which shall exercise the functions set out in Article 30;
Article 24, first paragraph, point (c)		
460	(c) an Executive Director who shall exercise the responsibilities set out in Article 32;	(c) an Executive Director who shall exercise the responsibilities set out in Article 32;

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 24, first paragraph, point (d)		
461	(d) a Deputy Executive Director who shall exercise the responsibilities set out in Article 34;	(d) a Deputy Executive Director who shall exercise the responsibilities set out in Article 34, *where the Management Board decides to create such a function in accordance with Article 33(2)*;
Article 24, first paragraph, point (e)		
462	(e) an ENISA Advisory Group;	(e) an ENISA Advisory Group;
Article 24, first paragraph, point (f)		
463	(f) a Board of Appeals which shall exercise the functions set out in Articles 39 to 42.	(f) a Board of Appeals which shall exercise the functions set out in Articles 39 to 42.
Section 1		
464	Section 1 Management Board	Section 1 Management Board
Article 25		
465	Article 25 Composition of the Management Board	Article 25 Composition of the Management Board
Article 25(1)		
466	1. The Management Board shall be composed of one member appointed by each Member State and two members appointed by the Commission. All members shall have the right to vote.	1. The Management Board shall be composed of one member appointed by each Member State and two members appointed by the Commission. All members shall have the right to vote.
Article 25(2)		
467	2. Each member of the Management Board shall have an alternate. The alternates shall represent the members in their absence.	2. Each member of the Management Board shall have an alternate. The alternates shall represent the members in their absence.
Article 25(3)		
468	3. Each Member State shall appoint the head of a national competent authority designated pursuant to Article 8(1) of Directive (EU) 2022/2555 as the member of the Management Board. Where this proves not to be feasible, Member States	3. Each Member State shall appoint *a representative with strategic decision-making power in the field of cybersecurity in the Member State as the member of the Management Board. Where possible this representative shall be* the head of a

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	shall appoint a high-level representative of a national competent authority designated pursuant to Article 8(1) of Directive (EU) 2022/2555 as the member of the Management Board.	~~national~~ competent authority designated pursuant to Article 8(1) of Directive (EU) 2022/2555 as the member of the Management Board. ~~Where this proves not to be feasible, Member States shall appoint a high-level representative of a national competent authority designated pursuant to Article 8(1) of Directive (EU) 2022/2555 as the member of the Management Board.~~
Article 25(4)		
469	4. Members appointed by the Commission and alternate members of the Management Board shall be appointed in light of their knowledge in the field of cybersecurity, taking into account their relevant managerial, administrative and budgetary skills. The Commission and the Member States as regards alternates, shall aim to achieve a balanced representation between men and women on the Management Board and shall make efforts to limit their turnover in order to ensure continuity of the Management Board's work.	4. Members appointed by the Commission and alternate members of the Management Board shall be appointed in light of their knowledge in the field of cybersecurity, taking into account their relevant managerial, administrative and budgetary skills. The Commission and the Member States as regards alternates, shall aim to achieve a balanced representation between men and women on the Management Board and shall make efforts to limit their turnover in order to ensure continuity of the Management Board's work.
Article 25(5)		
470	5. The term of office of the members appointed by Member States shall be equal to the term of their function referred to in paragraph 3.	5. ~~The term of office of the members appointed by Member States shall be equal to the term of their function referred to in paragraph 3.~~
Article 25(6)		
471	6. The term of office of the alternates and of the members appointed by the Commission shall be four years. That term shall be renewable.	6. The term of office of the ***members and their*** alternates ~~and of the members appointed by the Commission~~ shall be four years. That term shall be renewable.
Article 26		
472	Article 26 Chairperson of the Management Board	Article 26 Chairperson of the Management Board
Article 26(1)		
473	1. The Management Board shall elect a Chairperson and a Deputy Chairperson from among its members with voting rights. The Chairperson and the Deputy Chairperson shall be elected by a majority of two thirds of the members of the Management Board with voting rights.	1. The Management Board shall elect a Chairperson and a Deputy Chairperson from among its members ~~with voting rights~~. The Chairperson and the Deputy Chairperson shall be elected by a majority of two thirds of the members of the Management Board ~~with voting rights~~.

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 26(2)		
474	2. The Deputy Chairperson shall automatically replace the Chairperson if the Chairperson is prevented from attending to their duties.	2. The Deputy Chairperson shall automatically replace the Chairperson if the Chairperson is prevented from attending to their duties.
Article 26(3)		
475	3. The term of office of the Chairperson and of the Deputy Chairperson shall be four years and may be renewed once. If, however, their membership of the Management Board ends at any time during their term of office, that term of office shall automatically expire on that date.	3. The term of office of the Chairperson and of the Deputy Chairperson shall be four years and may be renewed once. If, however, their membership of the Management Board ends at any time during their term of office, that term of office shall automatically expire on that date.
Article 27		
476	Article 27 Meetings of the Management Board	Article 27 Meetings of the Management Board
Article 27(1)		
477	1. The Chairperson shall convene meetings of the Management Board.	1. The Chairperson shall convene meetings of the Management Board.
Article 27(2)		
478	2. The Executive Director shall take part in the meetings of the Management Board, without the right to vote.	2. The Executive Director shall take part in the meetings of the Management Board, without the right to vote.
Article 27(3)		
479	3. The Management Board shall hold at least two ordinary meetings a year. In addition, it shall meet on the initiative of its Chairperson, at the request of the Commission, or at the request of at least one third of its members.	3. The Management Board shall hold at least two ordinary meetings a year. In addition, it shall meet on the initiative of its Chairperson, at the request of the Commission, or at the request of at least one third of its members.
Article 27(4)		
480	4. A representative from the European Cybersecurity Industrial, Technology and Research Competence Centre established by Regulation (EU) 2021/887 shall be a permanent observer, without voting rights, at the meetings of the Management Board.	4. A representative from the European Cybersecurity Industrial, Technology and Research Competence Centre established by Regulation (EU) 2021/887 shall be a permanent observer, without voting rights, at the meetings of the Management Board.
Article 27(5)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
481	5. The Management Board may invite any person whose opinion may be of interest to attend a meeting, or part of a meeting, as an ad hoc observer, without voting rights and subject to the rules of procedure of the Management Board.	5. The Management Board may invite any person whose opinion may be of interest to attend a meeting, or part of a meeting, as an ad hoc observer, without voting rights and subject to the rules of procedure of the Management Board.
Article 27(6)		
482	6. The members of the Management Board and their alternates may be assisted at the meetings of the Management Board by advisers or experts, subject to the rules of procedure of the Management Board.	6. The members of the Management Board and their alternates may be assisted at the meetings of the Management Board by advisers or experts, subject to the rules of procedure of the Management Board.
Article 27(6a)		
482a		*6a. ENISA shall provide the secretariat of the Management Board.*
Article 28		
483	Article 28 Functions of the Management Board	Article 28 Functions of the Management Board
Article 28(1)		
484	1. The Management Board shall:	1. The Management Board shall:
Article 28(1), point (a)		
485	(a) establish the general direction of the operation of ENISA and ensure that ENISA operates in accordance with the rules and principles laid down in this Regulation; it shall also ensure the consistency of ENISA's work with activities conducted by the Member States as well as at Union level;	(a) establish the general direction of the operation of ENISA and ensure that ENISA operates in accordance with the rules and principles laid down in this Regulation; it shall also ensure the consistency of ENISA's work with activities conducted by the Member States as well as at Union level;
Article 28(1), point (b)		
486	(b) adopt ENISA's draft single programming document referred to in Article 44, before its submission to the Commission for an opinion;	(b) adopt ENISA's draft single programming document referred to in Article 44, before its submission to the Commission for an opinion;
Article 28(1), point (c)		
487	(c) taking into account the opinion of the Commission, adopt ENISA's single programming document in accordance with Article 29(2), point (a);	(c) ~~*taking into account the opinion of the Commission,*~~ adopt ENISA's single programming document in accordance with Article 29(2), point (a)*, taking into*

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
		account the opinion of the Commission;
Article 28(1), point (d)		
488	(d) supervise the implementation of the multiannual and annual programme included in the single programming document;	(d) supervise the implementation of the multiannual and annual programme included in the single programming document;
Article 28(1), point (e)		
489	(e) adopt the annual budget of ENISA in accordance with Article 29(2), point (b), and exercise other functions in respect of ENISA's budget in accordance with Chapter IV;	(e) adopt the annual budget of ENISA in accordance with Article 29(2), point (b), and exercise other functions in respect of ENISA's budget in accordance with Chapter IV;
Article 28(1), point (f)		
490	(f) assess and adopt the consolidated annual report on ENISA's activities, including the accounts and a description of how ENISA has met its performance indicators; submit both the annual report and the assessment thereof by 1 July of the following year to the European Parliament, to the Council, to the Commission and to the European Court of Auditors; make the annual report public;	(f) assess and adopt the consolidated annual report on ENISA's activities, including the accounts and a description of how ENISA has met its performance indicators; submit both the annual report and the assessment thereof by 1 July of the following year to the European Parliament, to the Council, to the Commission and to the European Court of Auditors; make the annual report public;
Article 28(1), point (g)		
491	(g) adopt the financial rules applicable to ENISA in accordance with Article 50;	(g) adopt the financial rules applicable to ENISA in accordance with Article 50;
Article 28(1), point (h)		
492	(h) adopt an anti-fraud strategy that is proportionate to the fraud risks, having regard to a cost-benefit analysis of the measures to be implemented;	(h) adopt an anti-fraud strategy that is proportionate to the fraud risks, having regard to a cost-benefit analysis of the measures to be implemented;
Article 28(1), point (ha)		
492a		*(ha)adopt a strategy for relations with stakeholders;* Linked to the amendments in Article 69(1a).
Article 28(1), point (hb)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
492b		*(hb) adopt a strategy for relations with third countries and international organisations pursuant to Article 70(2);*
Article 28(1), point (i)		
493	(i) ensure adequate follow-up to findings and recommendations stemming from internal or external audit reports and evaluations and from investigations of the European Anti-Fraud Office (OLAF) and of the European Public Prosecutor's Office (EPPO);	(i) ensure adequate follow-up to findings and recommendations stemming from internal or external audit reports and evaluations and from investigations of the European Anti-Fraud Office (OLAF) and of the European Public Prosecutor's Office (EPPO);
Article 28(1), point (j)		
494	(j) adopt its rules of procedure, including rules for provisional decisions on the delegation of specific tasks, pursuant to Article 30(7);	(j) adopt its rules of procedure, including rules for provisional decisions on the delegation of specific tasks, pursuant to Article 30(7);
Article 28(1), point (k)		
495	(k) exercise, in accordance with paragraph 2 of this Article, with respect to the staff of ENISA, the powers conferred by the Staff Regulations of Officials of the European Union (the 'Staff Regulations') and by the Conditions of Employment of Other Servants of the European Union (the 'Conditions of Employment'), laid down in Council Regulation (EEC, Euratom, ECSC) No 259/68[1], respectively, on the appointing authority and on the authority empowered to conclude a contract of employment ('appointing authority powers'); _____ 1. OJ L 56, 4.3.1968, p. 1, ELI: http://data.europa.eu/eli/reg/1968/259(1)/oj.	(k) exercise, in accordance with paragraph 2 of this Article, with respect to the staff of ENISA, the powers conferred by the Staff Regulations of Officials of the European Union (the 'Staff Regulations') and by the Conditions of Employment of Other Servants of the European Union (the 'Conditions of Employment'), laid down in Council Regulation (EEC, Euratom, ECSC) No 259/68[1], respectively, on the appointing authority and on the authority empowered to conclude a contract of employment ('appointing authority powers'); _____ 1. OJ L 56, 4.3.1968, p. 1, ELI: http://data.europa.eu/eli/reg/1968/259(1)/oj.
Article 28(1), point (l)		
496	(l) adopt implementing rules giving effect to the Staff Regulations and the Conditions of Employment in accordance with Article 110(2) of the Staff Regulations;	(l) adopt implementing rules giving effect to the Staff Regulations and the Conditions of Employment in accordance with Article 110(2) of the Staff Regulations;
Article 28(1), point (m)		
497	(m) appoint the Executive Director and, if it decides to create the function of a Deputy Executive Director, the Deputy Executive Director, and where relevant	(m) appoint the Executive Director and, if it decides to create the function of a Deputy Executive Director, the Deputy Executive Director, and where relevant

	CLEAN Commission Proposal	VS.EC Council Mandate
	extend their term of office or remove them from office in accordance with Article 31;	extend their term of office or remove them from office in accordance with Article 31;
Article 28(1), point (n)		
498	(n) appoint an accounting officer, subject to the Staff Regulations and the Conditions of Employment, who shall be independent in the performance of their duties;	(n) appoint an accounting officer, subject to the Staff Regulations and the Conditions of Employment, who shall be independent in the performance of their duties;
Article 28(1), point (o)		
499	(o) take all decisions concerning the establishment of ENISA's internal structures and, where necessary, the modification of those internal structures, taking into consideration ENISA's activity needs and having regard to sound budgetary management;	(o) take all decisions concerning the establishment of ENISA's internal structures and, where necessary, the modification of those internal structures, taking into consideration ENISA's activity needs and having regard to sound budgetary management;
Article 28(1), point (p)		
500	(p) authorise the conclusion of working arrangements with regard to Article 68;	(p) authorise the ~~conclusion of working~~*establishment of practical* arrangements with regard to Article 68;
Article 28(1), point (q)		
501	(q) authorise the conclusion of working arrangements in accordance with Article 70;	(q) authorise the ~~conclusion~~*establishment* of working arrangements in accordance with Article 70;
Article 28(1), point (r)		
502	(r) appoint and remove the members of the Board of Appeal in accordance with Article 29(2), point (d);	(r) appoint and remove the members of the Board of Appeal in accordance with Article 29(2), point (d);
Article 28(1), point (s)		
503	(s) adopt rules for the prevention and management of conflicts of interest in respect of the members of the Board of Appeal.	(s) adopt rules for the prevention and management of conflicts of interest in respect of the members of the Board of Appeal~~.~~*;* See Article 67 second subparagraph.
Article 28(1), point (sa)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
503a		*(sa) adopt the rules of procedure of the Executive Board.*
Article 28(2)		
504	2. In accordance with Article 110(2) of the Staff Regulations, the Management Board shall adopt a decision based on Article 2(1) of the Staff Regulations and Article 6 of the Conditions of Employment, delegating the relevant appointing authority powers to the Executive Director and defining the conditions under which that delegation of powers can be suspended. The Executive Director may sub-delegate those powers.	2. In accordance with Article 110(2) of the Staff Regulations, the Management Board shall adopt a decision based on Article 2(1) of the Staff Regulations and Article 6 of the Conditions of Employment, delegating the relevant appointing authority powers to the Executive Director and defining the conditions under which that delegation of powers can be suspended. The Executive Director may sub-delegate those powers.
Article 28(3)		
505	3. Where exceptional circumstances so require, the Management Board may adopt a decision to temporarily suspend the delegation of appointing authority powers to the Executive Director and any appointing authority powers sub-delegated by the Executive Director and instead exercise them itself or delegate them to one of its members or to a staff member other than the Executive Director.	3. Where exceptional circumstances so require, the Management Board may adopt a decision to temporarily suspend the delegation of appointing authority powers to the Executive Director and any appointing authority powers sub-delegated by the Executive Director and instead exercise them itself or delegate them to one of its members or to a staff member other than the Executive Director.
Article 29		
506	Article 29 Voting rules of the Management Board	Article 29 Voting rules of the Management Board
Article 29(1)		
507	1. The Management Board shall adopt its decisions by an absolute majority of its members with voting rights, except if otherwise provided in this Regulation.	1. The Management Board shall adopt its decisions by an absolute majority of its members with voting rights, except if otherwise provided in this Regulation.
Article 29(2)		
508	2. A majority of two thirds of the members of the Management Board with voting rights shall be required for:	2. A majority of two thirds of the members of the Management Board ~~*with voting rights*~~ shall be required for:
Article 29(2), point (a)		
509	(a) the adoption of the single programming document referred to in Article	(a) the adoption of the single programming document referred to in Article

	CLEAN Commission Proposal	VS.EC Council Mandate
	28(1)(c);	28(1)(c);
Article 29(2), point (b)		
510	(b) the adoption of the annual budget referred to in Article 28(1)(e);	(b) the adoption of the annual budget referred to in Article 28(1)(e);
Article 29(2), point (c)		
511	(c) the appointment, extension of the term of office or removal of the Executive Director and of the Deputy Executive Director, as referred to in Articles 31 and 33;	(c) the appointment, extension of the term of office or removal of the Executive Director and of the Deputy Executive Director, as referred to in Articles 31 and 33;
Article 29(2), point (d)		
512	(d) the appointment and removal of the members of the Board of Appeal, as referred to in Article 36.	(d) the appointment and removal of the members of the Board of Appeal, as referred to in Article 36.
Article 29(3)		
513	3. Decisions on budgetary or human resources matters, in particular matters referred to in Article 28(1), points (c), (e), (f), (g), (h), (i), (k), (l), (m), (n), shall only be adopted if the representatives of the Commission cast a positive vote. For the purposes of adopting the decisions referred to in Article 28(1), point (c) regarding ENISA's single programming document, a positive vote of the representative of the Commission shall only be required on the elements of the decision not related to the annual and multiannual work programme of ENISA.	3. ~~*Decisions on budgetary or human resources matters, in particular matters referred to in Article 28(1), points (c), (e), (f), (g), (h), (i), (k), (l), (m), (n), shall only be adopted if the representatives of the Commission cast a positive vote. For the purposes of adopting the decisions referred to in Article 28(1), point (c) regarding ENISA's single programming document, a positive vote of the representative of the Commission shall only be required on the elements of the decision not related to the annual and multiannual work programme of ENISA.*~~
Article 29(4)		
514	4. Each member with voting rights shall have one vote. In the absence of a member with the right to vote, their alternate shall be entitled to exercise the member's right to vote.	4. Each member ~~*with voting rights*~~ shall have one vote. In the absence of a member ~~*with the right to vote*~~, their alternate shall be entitled to exercise the member's right to vote.
Article 29(5)		
515	5. The Chairperson of the Management Board shall take part in the voting.	5. The Chairperson of the Management Board shall take part in the voting.
Article 29(6)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
516	6. The Executive Director shall not take part in the voting.	6. The Executive Director shall not take part in the voting.
Article 29(7)		
517	7. The Management Board's rules of procedure shall establish more detailed voting arrangements, in particular the circumstances in which a member may act on behalf of another member.	7. The Management Board's rules of procedure shall establish ~~more~~ detailed voting arrangements, in particular the circumstances in which a member may act on behalf of another member.
Section 2		
518	Section 2 Executive Board	Section 2 Executive Board
Article 30		
519	Article 30 Executive Board	Article 30 Executive Board
Article 30(1)		
520	1. The Management Board shall be assisted by an Executive Board.	1. The Management Board shall be assisted by an Executive Board.
Article 30(2)		
521	2. The Executive Board shall:	2. The Executive Board shall:
Article 30(2), point (a)		
522	(a) prepare decisions to be adopted by the Management Board;	(a) prepare decisions to be adopted by the Management Board;
Article 30(2), point (b)		
523	(b) together with the Management Board, ensure the adequate follow-up to findings and recommendations stemming from internal or external audit reports and evaluations, as well as from investigations of OLAF and the EPPO;	(b) together with the Management Board, ensure the adequate follow-up to findings and recommendations stemming from internal or external audit reports and evaluations, as well as from investigations of OLAF and the EPPO;
Article 30(2), point (c)		
524	(c) without prejudice to the responsibilities of the Executive Director set out in Article 32, assist and advise the Executive Director in implementing the decisions of the Management Board, with a view to reinforcing supervision of	(c) without prejudice to the responsibilities of the Executive Director set out in Article 32, assist and advise the Executive Director in implementing the decisions of the Management Board, with a view to reinforcing supervision of

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	administrative and budgetary management.	administrative and budgetary management.
Article 30(3)		
525	3. The Executive Board shall be composed of the Chairperson of the Management Board, one representative of the Commission to the Management Board, and three other members appointed by the Management Board from among its members with the right to vote. The Chairperson of the Management Board shall also be the Chairperson of the Executive Board. The appointments of the members of the Executive Board shall aim to ensure gender balance on the Executive Board. The Executive Director shall take part in the meetings of the Executive Board without the right to vote.	3. The Executive Board shall be composed of *five members. The members of the Executive Board shall be appointed from among the members of the Management Board. The members shall include* the Chairperson of the Management Board, one representative of the Commission to the Management Board, and three other members appointed by the Management Board from among its members ~~*with the right to vote*~~. The Chairperson of the Management Board shall also be the Chairperson of the Executive Board. The appointments of the members of the Executive Board shall aim to ensure gender balance on the Executive Board *and the broadest possible participation of Member States over time, including through a system of rotation*. The Executive Director shall take part in the meetings of the Executive Board without the right to vote.
Article 30(4)		
526	4. The term of office of the members of the Executive Board shall be four years. That term shall be renewable. The term of office of members of the Executive Board shall end when their membership of the Management Board ends.	4. The term of office of the members of the Executive Board *appointed by the Management Board pursuant to paragraph 3* shall be four years. That term shall be renewable *once*. The term of office of *those* members ~~*of the Executive Board*~~ shall end when their membership of the Management Board ends.
Article 30(5)		
527	5. The Executive Board shall hold at least one ordinary meeting every three months. In addition, it shall meet on the initiative of its Chairperson or at the request of its members.	5. The Executive Board shall hold at least one ordinary meeting every three months. In addition, it shall meet on the initiative of its Chairperson or at the request of its members.
Article 30(6)		
528	6. The Management Board shall lay down the rules of procedure of the Executive Board.	6. The Management Board shall lay down the rules of procedure of the Executive Board.
Article 30(7)		
529	7. When necessary due to urgency, the Executive Board may take certain	7. When necessary due to urgency, the Executive Board may take certain

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	provisional decisions on behalf of the Management Board, in particular on administrative management matters, including the suspension of the delegation of the appointing authority powers and budgetary matters. Any such provisional decisions shall be notified to the Management Board without undue delay. The Management Board shall then decide whether to approve or reject the provisional decision no later than three months after that decision was taken. The Executive Board shall not take decisions on behalf of the Management Board that require the approval of a majority of two thirds of the members of the Management Board with voting rights.	provisional decisions on behalf of the Management Board, in particular on administrative management matters, including the suspension of the delegation of the appointing authority powers and budgetary matters. Any such provisional decisions shall be notified to the Management Board without undue delay. The Management Board shall then decide whether to approve or reject the provisional decision no later than three months after that decision was taken. The Executive Board shall not take decisions on behalf of the Management Board that require the approval of a majority of two thirds of the members of the Management Board ~~with voting rights~~.
Section 3		
530	Section 3 Executive Director	Section 3 Executive Director
Article 31		
531	Article 31 Appointment, dismissal and extension of the term of office	Article 31 Appointment, dismissal and extension of the term of office
Article 31(1)		
532	1. The Executive Director shall be appointed by the Management Board on the basis of merit and skills from a list of candidates proposed by the Commission, following an open and transparent and selection procedure.	1. The Executive Director shall be appointed by the Management Board on the basis of merit and skills from a list of candidates proposed by the Commission, following an open and transparent and selection procedure.
Article 31(2)		
533	2. Before appointment, the candidate selected by the Management Board shall be invited to make a statement before the relevant committee of the European Parliament and to answer Members' questions.	2. Before appointment, the candidate selected by the Management Board shall be invited to make a statement before the relevant committee of the European Parliament and to answer Members' questions.
Article 31(3)		
534	3. The Executive Director shall be engaged as a temporary agent of ENISA under Article 2(a) of the Conditions of Employment.	3. The Executive Director shall be engaged as a temporary agent of ENISA under Article 2(a) of the Conditions of Employment.
Article 31(4)		

	CLEAN Commission Proposal	VS.EC Council Mandate
535	4.For the purpose of concluding the contract with the Executive Director, ENISA shall be represented by the Chairperson of the Management Board.	4.For the purpose of concluding the contract with the Executive Director, ENISA shall be represented by the Chairperson of the Management Board.
Article 31(5)		
536	5.The term of office of the Executive Director shall be five years. In due time before the end of that period, the Commission shall carry out an assessment that takes into account an evaluation of the performance of the Executive Director and ENISA's future tasks and challenges.	5.The term of office of the Executive Director shall be five years. In due time before the end of that period, the Commission shall carry out an assessment that takes into account an evaluation of the performance of the Executive Director and ENISA's future tasks and challenges.
Article 31(6)		
537	6.The Management Board, acting on a proposal from the Commission which takes into account the assessment referred to in paragraph 5, may extend the term of office of the Executive Director once for no more than five years.	6.The Management Board, ~~*acting on a proposal from the Commission which takes*~~*taking* into account the assessment referred to in paragraph 5, may extend the term of office of the Executive Director once for no more than five years.
Article 31(7)		
538	7.An Executive Director whose term of office has been extended may not participate in another selection procedure for the same post at the end of the overall period.	7.An Executive Director whose term of office has been extended may not participate in another selection procedure for the same post at the end of the overall period.
Article 31(8)		
539	8.The Management Board shall inform the European Parliament about its intention to extend the Executive Director's term of office in accordance with paragraph 6. Within three months before any such extension, the Executive Director, if invited, shall make a statement before the relevant committee of the European Parliament and answer members' questions.	8.The Management Board shall inform the European Parliament about its intention to extend the Executive Director's term of office in accordance with paragraph 6. Within three months before any such extension, the Executive Director, if invited, shall make a statement before the relevant committee of the European Parliament and answer members' questions.
Article 31(9)		
540	9.The Executive Director may be removed from office only upon a decision of the Management Board acting on a proposal from the Commission.	9.The Executive Director may be removed from office only upon a decision of the Management Board acting on a proposal from the Commission*, or from a third of the Management Board members*.
Article 32		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
541	Article 32 Tasks and responsibilities of the Executive Director	Article 32 Tasks and responsibilities of the Executive Director
Article 32(1)		
542	1. The Executive Director shall manage ENISA and shall be accountable to the Management Board.	1. The Executive Director shall manage ENISA and shall be accountable to the Management Board.
Article 32(2)		
543	2. The Executive Director shall be independent in the performance of their tasks and shall neither seek nor take instructions from any government nor from any other body.	2. The Executive Director shall be independent in the performance of their tasks and shall neither seek nor take instructions from any government nor from any other body.
Article 32(3)		
544	3. The Executive Director shall report to the European Parliament on the performance of their tasks when invited to do so. The Council may invite the Executive Director to report on the performance of their tasks.	3. The Executive Director shall report to the European Parliament on the performance of their tasks when invited to do so. The Council may invite the Executive Director to report on the performance of their tasks.
Article 32(4)		
545	4. The Executive Director shall be the legal representative of ENISA.	4. The Executive Director shall be the legal representative of ENISA.
Article 32(5)		
546	5. The Executive Director shall be responsible for the implementation of the tasks assigned to ENISA by this Regulation. In particular, the Executive Director shall:	5. The Executive Director shall be responsible for the implementation of the tasks assigned to ENISA by this Regulation. In particular, the Executive Director shall:
Article 32(5), point (a)		
547	(a) ensure the day-to-day administration of ENISA;	(a) ensure the day-to-day administration of ENISA;
Article 32(5), point (b)		
548	(b) implement decisions adopted by the Management Board;	(b) implement decisions adopted by the Management Board;
Article 32(5), point (c)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
549	(c) ensure compliance with the financial rules of ENISA;	(c) ensure compliance with the financial rules of ENISA;
Article 32(5), point (d)		
550	(d) prepare the draft single programming document and submit it to the Management Board for approval before its submission to the Commission for an opinion;	(d) prepare the draft single programming document and submit it to the Management Board for approval before its submission to the Commission for an opinion;
Article 32(5), point (e)		
551	(e) implement the single programming document and report to the Management Board on its implementation;	(e) implement the single programming document and report to the Management Board on its implementation;
Article 32(5), point (f)		
552	(f) prepare ENISA's consolidated annual activity report, including the implementation of ENISA's annual work programme, and present it to the Management Board for assessment and adoption;	(f) prepare ENISA's consolidated annual activity report, including the implementation of ENISA's annual work programme, and present it to the Management Board for assessment and adoption;
Article 32(5), point (g)		
553	(g) prepare an action plan that follows up on the conclusions of the retrospective evaluations of ENISA as referred to in Article 121, and reporting on progress every two years to the Commission;	(g) prepare an action plan that follows up on the conclusions of the retrospective evaluations of ENISA as referred to in Article 121, and reporting on progress every two years to the Commission;
Article 32(5), point (h)		
554	(h) prepare an action plan that follows up on conclusions of internal or external audit reports and evaluations, and from investigations of OLAF and of the EPPO and report on progress biannually to the Commission and regularly to the Management Board;	(h) prepare an action plan that follows up on conclusions of internal or external audit reports and evaluations, and from investigations of OLAF and of the EPPO and report on progress biannually to the Commission and regularly to the Management Board;
Article 32(5), point (i)		
555	(i) prepare the draft financial rules applicable to ENISA as referred to in Article 50;	(i) prepare the draft financial rules applicable to ENISA as referred to in Article 50;
Article 32(5), point (j)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
556	(j) prepare ENISA's draft statement of estimates of revenue and expenditure and implement its budget;	(j) prepare ENISA's draft statement of estimates of revenue and expenditure and implement its budget;
Article 32(5), point (k)		
557	(k) protect the financial interests of the Union by applying preventive measures against fraud, corruption and any other illegal activities, without prejudicing the investigative competence of OLAF and the EPPO, by effective checks and, if irregularities are detected, by recovering amounts wrongly paid and, where appropriate, by imposing effective, proportionate and dissuasive administrative and financial penalties;	(k) protect the financial interests of the Union by applying preventive measures against fraud, corruption and any other illegal activities, without prejudicing the investigative competence of OLAF and the EPPO, by effective checks and, if irregularities are detected, by recovering amounts wrongly paid and, where appropriate, by imposing effective, proportionate and dissuasive administrative and financial penalties;
Article 32(5), point (l)		
558	(l) prepare an anti-fraud strategy, an efficiency gains and synergies strategy, a strategy for cooperation with third countries or international organisations and a strategy for the organisational management and internal control systems for ENISA, and present it to the Management Board for approval;	(l) prepare an anti-fraud strategy, an efficiency gains and synergies strategy, a strategy for cooperation with third countries or international organisations and a strategy for the organisational management and internal control systems for ENISA, and present it to the Management Board for approval;
Article 32(5), point (m)		
559	(m) develop and maintain contact with the business community and consumers' organisations to ensure regular dialogue with relevant stakeholders;	(m) develop and maintain contact with the business community and consumers' organisations to ensure regular dialogue with relevant stakeholders;
Article 32(5), point (n)		
560	(n) exchange views and information regularly with relevant Union entities regarding their activities relating to cybersecurity to ensure coherence in the implementation of Union policy in that field;	(n) exchange views and information regularly with relevant Union entities regarding their activities relating to cybersecurity to ensure coherence in the implementation of Union policy in that field;
Article 32(5), point (o)		
561	(o) promote diversity and gender balance in the recruitment of ENISA's staff;	(o) promote diversity and gender balance in the recruitment of ENISA's staff;
Article 32(5), point (p)		
562	(p) adopt European individual cybersecurity skills attestation schemes, as referred to in Article 20(1);	(p) adopt European individual cybersecurity skills attestation schemes, as referred to in Article 20(1);

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 32(5), point (q)		
563	(q) adopt decisions with respect to applicants to become authorised attestation providers or to renew their authorisation, as referred to in Article 22(3);	(q) adopt decisions with respect to applicants to become authorised attestation providers or to renew their authorisation, as referred to in Article 22(3);
Article 32(5), point (r)		
564	(r) carry out other tasks assigned to the Executive Director by this Regulation.	(r) carry out other tasks assigned to the Executive Director by this Regulation.
Article 32(6)		
565	6. Where necessary and within ENISA's objectives and tasks, the Executive Director may set up ad hoc working groups composed of experts, including experts from the Member States' competent authorities. The Executive Director shall inform the Management Board in advance thereof. The procedures regarding in particular the composition of the working groups, the appointment of the experts of the working groups by the Executive Director and the operation of the working groups shall be specified in ENISA's internal rules of operation.	6. Where necessary and within ENISA's objectives and tasks, the Executive Director may set up ad hoc working groups composed of experts, including experts from the Member States' competent authorities. The Executive Director shall inform the Management Board in advance thereof. The procedures regarding in particular the composition of the working groups, the appointment of the experts of the working groups by the Executive Director and the operation of the working groups shall be specified in ENISA's internal rules of operation.
Article 32(7)		
566	7. Where necessary for the purpose of carrying out ENISA's tasks in an efficient and effective manner and based on an appropriate cost-benefit analysis, the Executive Director may decide to establish one or more local offices in one or more Member States. Before deciding to establish a local office, the Executive Director shall seek the opinion of the Member States concerned, including the Member State in which the seat of ENISA is located, and shall obtain the prior consent of the Commission and the Management Board. In cases of disagreement during the consultation process between the Executive Director and the Member States concerned, the issue shall be brought to the Council for discussion. The aggregate number of staff in all local offices shall be kept to a minimum and shall not exceed 40% of the total number of ENISA's staff located in the Member State in which the seat of ENISA is located. The number of the staff in each local office shall not exceed 10% of the total number of ENISA's staff located in the Member State in which the seat of ENISA is located.	7. Where necessary for the purpose of carrying out ENISA's tasks in an efficient and effective manner and based on an appropriate cost-benefit analysis, the Executive Director may decide to establish one or more local offices in one or more Member States. Before deciding to establish a local office, the Executive Director shall seek the opinion of the Member States concerned, including the Member State in which the seat of ENISA is located, and shall obtain the prior consent of the Commission and the Management Board. In cases of disagreement during the consultation process between the Executive Director and the Member States concerned, the issue shall be brought to the Council for discussion. The aggregate number of staff in all local offices shall be kept to a minimum and shall not exceed 40% of the total number of ENISA's staff located in the Member State in which the seat of ENISA is located. The number of the staff in each local office shall not exceed 10% of the total number of ENISA's staff located in the Member State in which the seat of ENISA is located.

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 32(8)		
567	8. The decision establishing a local office shall specify the scope of the activities to be carried out at the local office in a manner that avoids unnecessary costs and duplication of administrative functions of ENISA.	8. The decision establishing a local office shall specify the scope of the activities to be carried out at the local office in a manner that avoids unnecessary costs and duplication of administrative functions of ENISA.
Section 4		
568	Section 4 Deputy Executive Director	Section 4 Deputy Executive Director
Article 33		
569	Article 33 Deputy Executive Director	Article 33 Deputy Executive Director
Article 33(1)		
570	1. The Management Board may decide to create a function of a Deputy Executive Director to assist the Executive Director.	1. The Management Board may decide to create a function of a Deputy Executive Director to assist the Executive Director. *Before taking the decision the Executive Director shall be given the opportunity to issue a reasoned opinion, which shall be taken into consideration by the Management Board.*
Article 33(2)		
571	2. Where the Management Board decides to create a function of a Deputy Executive Director, the provisions of Article 31 shall apply to the Deputy Executive Director accordingly.	2. Where the Management Board decides to create a function of a Deputy Executive Director, the provisions of Article 31 shall apply to the Deputy Executive Director accordingly.
Article 34		
572	Article 34 Tasks and responsibilities of the Deputy Executive Director	Article 34 Tasks and responsibilities of the Deputy Executive Director
Article 34, first paragraph		
573	The Deputy Executive Director shall assist the Executive Director in managing ENISA and in carrying out the tasks referred to in Article 32. If the Executive Director is absent or indisposed, or the post is vacant, the Deputy Executive Director shall take their place during the time of absence or until the post is filled.	The Deputy Executive Director shall assist the Executive Director in managing ENISA and in carrying out the tasks referred to in Article 32. *The Executive Director shall set out the tasks and responsibilities of the Deputy Executive Director*. If the Executive Director is absent or indisposed, or the post is vacant,

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
		the Deputy Executive Director shall take their place during the time of absence or until the post is filled.
Section 5		
574	Section 5 ENISA Advisory Group	Section 5 ENISA Advisory Group
Article 35		
575	Article 35 ENISA Advisory Group	Article 35 ENISA Advisory Group
Article 35(1)		
576	1. The Management Board, acting on a proposal from the Executive Director, shall establish in a transparent manner the ENISA Advisory Group. The ENISA Advisory Group shall be composed of recognised experts representing relevant stakeholders, such as the cybersecurity industry, ICT industry, SMEs, entities operating in sectors listed in Annexes I and II to Directive (EU) 2022/2555, manufacturers of products with digital elements and open-source software stewards within the meaning of Regulation (EU) 2024/2847, conformity assessment bodies notified under the European Cybersecurity Certification Framework referred to in Article 93 and Regulation (EU) 2024/2847, entities operating in the area of electronic identification means, consumer groups, academic experts in the field of cybersecurity, European standardisation organisations, as well as law enforcement and data protection supervisory authorities. Those recognised experts shall be nationals of Member States. The Management Board shall aim to ensure an appropriate gender and geographical balance, as well as a balance between the different stakeholder groups.	1. The Management Board, acting on a proposal from the Executive Director, shall establish in a transparent manner the ENISA Advisory Group. The ENISA Advisory Group shall be composed of recognised experts representing relevant stakeholders, such as the cybersecurity industry, ICT industry, SMEs, entities operating in sectors listed in Annexes I and II to Directive (EU) 2022/2555, manufacturers of products with digital elements and open-source software stewards within the meaning of Regulation (EU) 2024/2847, conformity assessment bodies notified under the European Cybersecurity Certification Framework referred to in Article 93 and Regulation (EU) 2024/2847, entities operating in the area of electronic identification means, consumer groups, academic experts in the field of cybersecurity, European standardisation organisations, as well as law enforcement and data protection supervisory authorities. Those recognised experts shall be nationals of Member States. The Management Board shall aim to ensure an appropriate gender and geographical balance, as well as a balance between the different stakeholder groups.
Article 35(2)		
577	2. Procedures for the ENISA Advisory Group, in particular regarding its composition, the proposal by the Executive Director referred to in paragraph 1, the number and appointment of its members and the operation of the ENISA	2. Procedures for the ENISA Advisory Group, in particular regarding its composition, the proposal by the Executive Director referred to in paragraph 1, the number and appointment of its members and the operation of the ENISA

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	Advisory Group, shall be specified in ENISA's internal rules of operation and shall be made public.	Advisory Group, shall be specified in ENISA's internal rules of operation and shall be made public.
Article 35(3)		
578	3. The ENISA Advisory Group shall be chaired by the Executive Director or by any person whom the Executive Director appoints on a case-by-case basis.	3. The ENISA Advisory Group shall be chaired by the Executive Director or by any person whom the Executive Director appoints on a case-by-case basis.
Article 35(4)		
579	4. The term of office of the members of the ENISA Advisory Group shall be two and a half years and shall be renewable once. Members of the Management Board shall not be members of the ENISA Advisory Group. Experts from the Commission and experts from the Member States shall be entitled to be present at the meetings of the ENISA Advisory Group and to participate in its work. The Executive Director may invite representatives of other bodies that are not members of the ENISA Advisory Group, to attend the meetings of the ENISA Advisory Group and to participate in its work.	4. The term of office of the members of the ENISA Advisory Group shall be two and a half years and shall be renewable once. Members of the Management Board shall not be members of the ENISA Advisory Group. Experts from the Commission and experts from the Member States shall be entitled to be present at the meetings of the ENISA Advisory Group and to participate in its work. The Executive Director may invite representatives of other bodies that are not members of the ENISA Advisory Group, to attend the meetings of the ENISA Advisory Group and to participate in its work.
Article 35(5)		
580	5. The ENISA Advisory Group shall advise ENISA in respect of the performance of ENISA's tasks, except for the application of the provisions of Titles III, IV and V of this Regulation. It shall in particular advise the Executive Director on the drawing up of a proposal for ENISA's annual work programme, and on ensuring communication with the relevant stakeholders on issues related to the annual work programme.	5. The ENISA Advisory Group shall advise ENISA in respect of the performance of ENISA's tasks, except for the application of the provisions of Titles III, IV and V of this Regulation. It shall in particular advise the Executive Director on the drawing up of a proposal for ENISA's annual work programme, and on ensuring communication with the relevant stakeholders on issues related to the annual work programme.
Article 35(6)		
581	6. The ENISA Advisory Group shall inform the Management Board of its activities on a regular basis.	6. The ENISA Advisory Group shall inform the Management Board of its activities on a regular basis.
Article 35(7)		
582	7. ENISA shall provide the logistical support necessary for the ENISA Advisory Group and provide a secretariat for its meetings.	7. ENISA shall provide the logistical support necessary for the ENISA Advisory Group and provide a secretariat for its meetings.

PUBLIC

	CLEAN	Commission Proposal	VS.EC	Council Mandate
Section 6				
583		Section 6 Board of Appeal		Section 6 Board of Appeal
Article 36				
584		Article 36 Creation and composition of the Board of Appeal		Article 36 Creation and composition of the Board of Appeal
Article 36(1)				
585		1. ENISA shall establish a Board of Appeal by a decision of the Management Board.		1. ENISA shall establish a Board of Appeal by a decision of the Management Board.
Article 36(2)				
586		2. The Board of Appeal shall be composed of a Chairperson and three other members. Each member of the Board of Appeal shall have an alternate. The alternate shall represent the member in their absence.		2. The Board of Appeal shall be composed of a Chairperson and three other members. Each member of the Board of Appeal shall have an alternate. The alternate shall represent the member in their absence.
Article 36(3)				
587		3. The Management Board shall appoint the Chairperson, the other members and their alternates from a list of qualified candidates established by the Commission. The list of qualified candidates shall be valid for four years. The validity of this list may be extended by the Management Board for additional four-year periods acting on a proposal from the Commission.		3. The Management Board shall appoint the Chairperson, the other members and their alternates from a list of qualified candidates established by the Commission. *The candidates shall be nationals of Member States*. The list of qualified candidates shall be valid for four years. The validity of this list may be extended by the Management Board for additional four-year periods acting on a proposal from the Commission.
Article 36(3a)				
587a				*3a. The appointments of the members of the Board of Appeal shall aim to ensure gender balance and the broadest possible participation of Member States over time.*
Article 36(4)				
588		4. Where the Board of Appeal considers that the nature of the appeal so requires, it may request the Management Board to appoint two additional members and		4. Where the Board of Appeal considers that the nature of the appeal so requires, it may request the Management Board to appoint two additional members and

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	their alternates from the list referred to in paragraph 3.	their alternates from the list referred to in paragraph 3.
Article 36(5)		
589	5. The Board of Appeal shall adopt and make public its rules of procedure.	5. The Board of Appeal shall adopt and make public its rules of procedure.
Article 37		
590	Article 37 Members of the Board of Appeal	Article 37 Members of the Board of Appeal
Article 37(1)		
591	1. The term of office of the members and alternates of the Board of Appeal shall be four years. Their term of office may be renewed by the Management Board for additional four-year periods acting on a proposal from the Commission.	1. The term of office of the members and alternates of the Board of Appeal shall be four years. Their term of office may be renewed by the Management Board for additional four-year periods acting on a proposal from the Commission.
Article 37(2)		
592	2. The members of the Board of Appeal shall be independent and shall not perform any other duties within ENISA. In making their decisions they shall neither seek nor take instructions from any government, any other body or any private entity.	2. The members of the Board of Appeal shall be independent and shall not perform any other duties within ENISA. In making their decisions they shall neither seek nor take instructions from any government, any other body or any private entity.
Article 37(3)		
593	3. The members of the Board of Appeal shall not be removed from office or from the list of qualified candidates during their term of office, unless there are serious grounds for such removal and the Management Board takes a decision to that effect, acting on a proposal from the Commission.	3. The members of the Board of Appeal shall not be removed from office or from the list of qualified candidates during their term of office, unless there are serious grounds for such removal and the Management Board takes a decision to that effect, acting on a proposal from the Commission.
Article 38		
594	Article 38 Exclusion and objection	Article 38 Exclusion and objection
Article 38(1)		
595	1. The members of the Board of Appeal shall not take part in any appeal	1. The members of the Board of Appeal shall not take part in any appeal

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	proceedings if they have any personal interest in the proceedings, if they have previously been involved as representatives of one of the parties to the proceedings, or if they participated in the adoption of the decision under appeal.	proceedings if they have any personal interest in the proceedings, if they have previously been involved as representatives of one of the parties to the proceedings, or if they participated in the adoption of the decision under appeal.
Article 38(2)		
596	2. If, for one of the reasons listed in paragraph 1 or for any other reason, a member of a Board of Appeal considers that they should not take part in any appeal proceeding, they shall inform the Board of Appeal accordingly.	2. If, for one of the reasons listed in paragraph 1 or for any other reason, a member of a Board of Appeal considers that they should not take part in any appeal proceeding, they shall inform the Board of Appeal accordingly.
Article 38(3)		
597	3. A party to the appeal proceedings may object to any member of a Board of Appeal on any of the grounds listed in paragraph 1, or if the member is suspected of partiality. Any such objection shall not be admissible if, while being aware of a reason for objecting, the party to the appeal proceedings has taken a procedural step. No objection may be based on the nationality of members of the Board of Appeal.	3. A party to the appeal proceedings may object to any member of a Board of Appeal on any of the grounds listed in paragraph 1, or if the member is suspected of partiality. Any such objection shall not be admissible if, while being aware of a reason for objecting, the party to the appeal proceedings has taken a procedural step. No objection may be based on the nationality of members of the Board of Appeal.
Article 38(4)		
598	4. The Board of Appeal shall decide as to the action to be taken in the cases specified in paragraphs 2 and 3 without the participation of the member concerned. For the purposes of taking that decision, the member concerned shall be replaced on the Board of Appeal by their alternate.	4. The Board of Appeal shall decide as to the action to be taken in the cases specified in paragraphs 2 and 3 without the participation of the member concerned. For the purposes of taking that decision, the member concerned shall be replaced on the Board of Appeal by their alternate.
Article 39		
599	Article 39 Appeals against decisions and failures to act	Article 39 Appeals against decisions and failures to act
Article 39(1)		
600	1. An appeal may be brought before the Board of Appeal against:	1. An appeal may be brought before the Board of Appeal against:
Article 39(1), point (a)		
601	(a) decisions adopted by ENISA pursuant to Article 22(3);	(a) decisions adopted by ENISA pursuant to Article 22(3);

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 39(1), point (b)		
602	(b) ENISA's failure to act within the applicable time limits laid down in Article 22(4).	(b) ENISA's failure to act within the applicable time limits laid down in Article 22(4).
Article 39(2)		
603	2. An appeal brought pursuant to paragraph 1 shall be subject to interlocutory revision in accordance with Article 41 before being put to the Board of Appeal for examination.	2. An appeal brought pursuant to paragraph 1 shall be subject to interlocutory revision in accordance with Article 41 before being put to the Board of Appeal for examination.
Article 39(3)		
604	3. An appeal brought pursuant to paragraph 1 shall not have a suspensive effect.	3. An appeal brought pursuant to paragraph 1 shall not have a suspensive effect.
Article 40		
605	Article 40 Persons entitled to appeal, time limit and form	Article 40 Persons entitled to appeal, time limit and form
Article 40(1)		
606	1. Applicants within the meaning of Article 21(3) may appeal against	1. Applicants within the meaning of Article 21(3) may appeal against
Article 40(1), point (a)		
607	(a) a decision of ENISA addressed to them, pursuant to Article 22(3);	(a) a decision of ENISA addressed to them, pursuant to Article 22(3);
Article 40(1), point (b)		
608	(b) ENISA's failure to act in respect of an application submitted by them to ENISA within the applicable time limits laid down in Article 22(4).	(b) ENISA's failure to act in respect of an application submitted by them to ENISA within the applicable time limits laid down in Article 22(4).
Article 40(2)		
609	2. In the case referred to in paragraph 1, point (a), the appeal, together with the statement of grounds thereof, shall be filed in writing in accordance with the rules of procedure referred to in Article 36(5) within two months of notification of the decision to the applicant concerned, or, in the absence thereof, of the day on which the decision came to the knowledge of the applicant.	2. In the case referred to in paragraph 1, point (a), the appeal, together with the statement of grounds thereof, shall be filed in writing in accordance with the rules of procedure referred to in Article 36(5) within two months of notification of the decision to the applicant concerned, or, in the absence thereof, of the day on which the decision came to the knowledge of the applicant.

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 40(3)		
610	3.In the case referred to in paragraph 1, point (b), the appeal shall be filed with ENISA in writing in accordance with the rules of procedure referred to in Article 36(5) within two months of the day of expiry of the time limit set out in Article 22(4).	3.In the case referred to in paragraph 1, point (b), the appeal shall be filed with ENISA in writing in accordance with the rules of procedure referred to in Article 36(5) within two months of the day of expiry of the time limit set out in Article 22(4).
Article 41		
611	Article 41 Interlocutory revision	Article 41 Interlocutory revision
Article 41(1)		
612	1.If ENISA considers the appeal to be admissible and well founded, it shall rectify the decision or failure to act referred to in Article 40(1).	1.If ENISA considers the appeal to be admissible and well founded, it shall rectify the decision or failure to act referred to in Article 40(1).
Article 41(2)		
613	2.If ENISA does not rectify the decision within one month after receipt of the appeal, it shall immediately decide whether to suspend the application of its decision and shall refer the appeal to the Board of Appeal.	2.If ENISA does not rectify the decision within one month after receipt of the appeal, it shall immediately decide whether to suspend the application of its decision and shall refer the appeal to the Board of Appeal.
Article 42		
614	Article 42 Examination of decisions on appeals	Article 42 Examination of decisions on appeals
Article 42(1)		
615	1.The Board of Appeal shall decide within three months of the appeal being filed whether to grant or refuse that appeal. When examining an appeal, the Board of Appeal shall act within the deadlines laid down in its rules of procedure. It shall, as often as necessary, invite the parties to the appeal proceedings to file, within specified time limits, observations on its notifications or on communications from other parties to the appeal proceedings. Parties to the appeal proceedings shall be entitled to make oral representations.	1.The Board of Appeal shall decide within three months of the appeal being filed whether to grant or refuse that appeal. When examining an appeal, the Board of Appeal shall act within the deadlines laid down in its rules of procedure. It shall, as often as necessary, invite the parties to the appeal proceedings to file, within specified time limits, observations on its notifications or on communications from other parties to the appeal proceedings. Parties to the appeal proceedings shall be entitled to make oral representations.

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 42(2)		
616	2.Where the Board of Appeal finds that the grounds for appeal are founded, it shall remit the case to ENISA. ENISA shall take its final decision in compliance with the findings of the Board of Appeal and shall provide a statement of reasons for that decision. ENISA shall inform the parties to the appeal proceedings accordingly.	2.Where the Board of Appeal finds that the grounds for appeal are founded, it shall remit the case to ENISA. ENISA shall take its final decision in compliance with the findings of the Board of Appeal and shall provide a statement of reasons for that decision. ENISA shall inform the parties to the appeal proceedings accordingly.
Article 43		
617	Article 43 Actions before the Court of Justice of the European Union	Article 43 Actions before the Court of Justice of the European Union
Article 43(1)		
618	1.Actions for the annulment of decisions of ENISA adopted pursuant to Article 22(3), or actions for failure to act within the applicable time limits pursuant to Article 22(4), may be brought before the Court of Justice of the European Union, after the appeal procedure within ENISA laid down in Articles 39 to 42 has been exhausted or in the event of failure to act within the applicable time limit pursuant to Article 41(2).	1.Actions for the annulment of decisions of ENISA adopted pursuant to Article 22(3), or actions for failure to act within the applicable time limits pursuant to Article 22(4), may be brought before the Court of Justice of the European Union, after the appeal procedure within ENISA laid down in Articles 39 to 42 has been exhausted or in the event of failure to act within the applicable time limit pursuant to Article 41(2).
Article 43(2)		
619	2.ENISA shall take all necessary measures to comply with the judgment of the Court of Justice of the European Union.	2.ENISA shall take all necessary measures to comply with the judgment of the Court of Justice of the European Union.
Section 7		
620	Section 7 Operations	Section 7 Operations
Article 44		
621	Article 44 Single programming document	Article 44 Single programming document
Article 44(1)		
622	1.ENISA shall operate in accordance with a single programming document	1.ENISA shall operate in accordance with a single programming document

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	containing its annual and multiannual work programme, which shall include all of its planned activities.	containing its annual and multiannual work programme, which shall include all of its planned activities.
Article 44(2)		
623	2. Each year, the Executive Director shall draw up a draft single programming document, as referred to in paragraph 1, with the corresponding financial and human resources planning in accordance with Article 32 of Commission Delegated Regulation (EU) 2019/715[1] and taking into account the guidelines set by the Commission. _____ 1. Commission Delegated Regulation (EU) 2019/715 of 18 December 2018 on the framework financial regulation for the bodies set up under the TFEU and Euratom Treaty and referred to in Article 70 of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council (OJ L 122, 10.5.2019, p. 1, ELI: http://data.europa.eu/eli/reg_del/2019/715/oj).	2. Each year, the Executive Director shall draw up a draft single programming document, as referred to in paragraph 1, with the corresponding financial and human resources planning in accordance with Article 32 of Commission Delegated Regulation (EU) 2019/715[1] and taking into account the guidelines set by the Commission. _____ 1. Commission Delegated Regulation (EU) 2019/715 of 18 December 2018 on the framework financial regulation for the bodies set up under the TFEU and Euratom Treaty and referred to in Article 70 of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council (OJ L 122, 10.5.2019, p. 1, ELI: http://data.europa.eu/eli/reg_del/2019/715/oj). See also Article 32(4)(d) on tasks of the Executive Director.
Article 44(3)		
624	3. By 30 November each year, the Management Board shall adopt the single programming document referred to in paragraph 1, taking into account the opinion of the Commission referred to in Article 32(7) of Delegated Regulation (EU) 2019/715. If the Management Board decides not to take into account any elements of the opinion of the Commission, it shall provide thorough justification for that decision. The Management Board shall forward the single programming document to the European Parliament, to the Council and to the Commission by 31 January of the following year, as well as any subsequently updated versions of that document.	3. By 30 November each year, the Management Board shall adopt the single programming document referred to in paragraph 1, taking into account the opinion of the Commission referred to in Article 32(7) of Delegated Regulation (EU) 2019/715. If the Management Board ~~*decides not to*~~ ***does not fully*** take into account ~~*any elements of*~~ the opinion of the Commission, it shall provide ~~*thorough justification*~~ ***adequate explanations*** for that decision. The Management Board shall forward the single programming document to the European Parliament, to the Council and to the Commission by 31 January of the following year, as well as any subsequently updated versions of that document. Aligned to the wording of Article 32(7) of Delegated Regulation.
Article 44(4)		
625	4. The single programming document shall become final after the definitive	4. The single programming document shall become final after the definitive

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	adoption of the general budget of the Union and shall be adjusted as necessary.	adoption of the general budget of the Union and shall be adjusted *by the Management Board* as necessary.
Article 44(5)		
626	5. The annual work programme shall comprise detailed objectives and expected results including performance indicators. It shall also contain a description of the actions to be financed and an indication of the financial and human resources allocated to each action, in accordance with the principles of activity-based budgeting and management. The annual work programme shall be coherent with the multiannual work programme referred to in paragraph 7. It shall clearly indicate tasks that have been added, changed or deleted in comparison with the previous financial year.	5. The annual work programme shall comprise detailed objectives and expected results including performance indicators. It shall also contain a description of the actions to be financed and an indication of the financial and human resources allocated to each action, in accordance with the principles of activity-based budgeting and management. The annual work programme shall be coherent with the multiannual work programme referred to in paragraph 7. It shall clearly indicate tasks that have been added, changed or deleted in comparison with the previous financial year.
Article 44(6)		
627	6. The Management Board shall amend the adopted annual work programme when a new task is assigned to ENISA. Any substantial amendments to the annual work programme shall be adopted by the same procedure as for the initial annual work programme. The Management Board may delegate the power to make non-substantial amendments to the annual work programme to the Executive Director.	6. The Management Board shall amend the adopted annual work programme when a new task is assigned to ENISA. Any substantial amendments to the annual work programme shall be adopted by the same procedure as for the initial annual work programme. The Management Board may delegate the power to make non-substantial amendments to the annual work programme to the Executive Director.
Article 44(7)		
628	7. The multiannual work programme shall set out the overall strategic programming including objectives, expected results and performance indicators. It shall also set out the resource programming including multiannual budget and staff.	7. The multiannual work programme shall set out the overall strategic programming including objectives, expected results and performance indicators. It shall also set out the resource programming including multiannual budget and staff.
Article 44(8)		
629	8. The resource programming shall be updated annually. The strategic programming shall be updated where appropriate and in particular where necessary to address the outcome of the evaluation referred to in Article 120.	8. The resource programming shall be updated annually. The strategic programming shall be updated where appropriate and in particular where necessary to address the outcome of the evaluation referred to in Article 120.

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
CHAPTER IV		
630	CHAPTER IV Establishment and structure of ENISA's budget	CHAPTER IV Establishment and structure of ENISA's budget
Article 45		
631	Article 45 Establishment of ENISA's budget	Article 45 Establishment of ENISA's budget
Article 45(1)		
632	1. Each year, the Executive Director shall draw up a provisional draft estimate of ENISA's revenue and expenditure for the following financial year, including the establishment plan, and shall send it to the Management Board.	1. Each year, the Executive Director shall draw up a provisional draft estimate of ENISA's revenue and expenditure for the following financial year, including the establishment plan, and shall send it to the Management Board.
Article 45(2)		
633	2. The provisional draft estimate shall be based on the objectives and expected results of the annual work programme, and shall take into account the financial resources necessary to achieve those objectives and expected results, in accordance with the principle of sound financial management and performance.	2. The provisional draft estimate shall be based on the objectives and expected results of the annual work programme, and shall take into account the financial resources necessary to achieve those objectives and expected results, in accordance with the principle of sound financial management and performance.
Article 45(3)		
634	3. On the basis of the provisional draft estimate, the Management Board shall adopt a draft estimate of ENISA's revenue and expenditure for the following financial year, and shall send it to the Commission by 31 January each year.	3. On the basis of the provisional draft estimate, the Management Board shall adopt a draft estimate of ENISA's revenue and expenditure for the following financial year, and shall send it to the Commission by 31 January each year.
Article 45(4)		
635	4. The Commission shall send the draft estimate to the budgetary authority together with the draft general budget of the Union. The draft estimate shall also be made available to ENISA.	4. The Commission shall send the draft estimate to the budgetary authority together with the draft general budget of the Union. The draft estimate shall also be made available to ENISA.
Article 45(5)		
636	5. On the basis of the draft estimate, the Commission shall enter in the draft general budget of the Union the estimates it considers to be necessary for the	5. On the basis of the draft estimate, the Commission shall enter in the draft general budget of the Union the estimates it considers to be necessary for the

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	establishment plan and the amount of the contribution to be charged to the general budget of the Union, which it shall submit to the budgetary authority in accordance with Articles 313 and 314 TFEU.	establishment plan and the amount of the contribution to be charged to the general budget of the Union, which it shall submit to the budgetary authority in accordance with Articles 313 and 314 TFEU.
Article 45(6)		
637	6. The budgetary authority shall authorise the appropriations for the contribution from the general budget of the Union to ENISA.	6. The budgetary authority shall authorise the appropriations for the contribution from the general budget of the Union to ENISA.
Article 45(7)		
638	7. The budgetary authority shall adopt ENISA's establishment plan.	7. The budgetary authority shall adopt ENISA's establishment plan.
Article 45(8)		
639	8. The Management Board shall adopt ENISA's budget. It shall become final following the final adoption of the general budget of the Union, and, if necessary, it shall be adjusted accordingly.	8. The Management Board shall adopt ENISA's budget. It shall become final following the final adoption of the general budget of the Union, and, if necessary, it shall be adjusted accordingly.
Article 45(9)		
640	9. For any building project likely to have significant implications for the budget of ENISA, Delegated Regulation (EU) 2019/715 shall apply.	9. For any building project likely to have significant implications for the budget of ENISA, Delegated Regulation (EU) 2019/715 shall apply.
Article 46		
641	Article 46 Structure of ENISA's budget	Article 46 Structure of ENISA's budget
Article 46(1)		
642	1. Estimates of all revenue and expenditure of ENISA shall be prepared each financial year and shall be shown in ENISA's budget. The financial year shall correspond to the calendar year.	1. Estimates of all revenue and expenditure of ENISA shall be prepared each financial year and shall be shown in ENISA's budget. The financial year shall correspond to the calendar year.
Article 46(2)		
643	2. ENISA's budget shall be balanced in terms of revenue and expenditure.	2. ENISA's budget shall be balanced in terms of revenue and expenditure.
Article 46(3)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
644	3. Without prejudice to other resources, ENISA's revenue shall be composed of:	3. Without prejudice to other resources, ENISA's revenue shall be composed of:
Article 46(3), point (a)		
645	(a) a contribution from the Union entered in the general budget of the Union;	(a) a contribution from the Union entered in the general budget of the Union;
Article 46(3), point (b)		
646	(b) revenue assigned to specific items of expenditure in accordance with its financial rules referred to in Article 50;	(b) revenue assigned to specific items of expenditure in accordance with its financial rules referred to in Article 50;
Article 46(3), point (c)		
647	(c) Union funding in the form of contribution agreements or ad hoc grants in accordance with ENISA's financial rules referred to in Article 50 and with the provisions of the relevant instruments supporting the policies of the Union;	(c) Union funding in the form of contribution agreements or ad hoc grants in accordance with ENISA's financial rules referred to in Article 50 and with the provisions of the relevant instruments supporting the policies of the Union;
Article 46(3), point (d)		
648	(d) the fees levied on the applicants for activities related to European individual cybersecurity skills attestation schemes referred to in Article 22(1);	(d) the fees levied on the applicants for activities related to European individual cybersecurity skills attestation schemes referred to in Article 22(1);
Article 46(3), point (e)		
649	(e) the fees levied on the conformity assessment bodies for participation in and issuance of European cybersecurity certificates under a European cybersecurity certification scheme referred to in Article 47(2);	(e) the fees levied on the conformity assessment bodies for participation in and issuance of European cybersecurity certificates under a European cybersecurity certification scheme referred to in Article 47(2);
Article 46(3), point (f)		
650	(f) the fees levied on public authorities or private bodies for testing tools as referred to in Article 47(3);	(f) the fees levied on public authorities or private bodies for testing tools as referred to in Article 47(3);
Article 46(3), point (g)		
651	(g) any contribution from third countries participating in the work of ENISA, as provided for in Article 70(4);	(g) any contribution from third countries participating in the work of ENISA, as provided for in Article 70(4);
Article 46(3), point (h)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
652	(h) any voluntary contributions from Member States in money or in kind.	(h) any voluntary contributions from Member States in money or in kind.
Article 46(4)		
653	4. Member States that provide voluntary contributions, as referred to in paragraph 3, point (g) shall not claim any specific right or service as a result thereof.	4. Member States that provide voluntary contributions, as referred to in paragraph 3, point ~~(g)~~ **(h)** shall not claim any specific right or service as a result thereof.
Article 46(5)		
654	5. The expenditure of ENISA shall include staff remuneration, administrative and infrastructure expenses, and operational expenditure.	5. The expenditure of ENISA shall include staff remuneration, administrative and infrastructure expenses, and operational expenditure.
Article 47		
655	Article 47 Fees	Article 47 Fees
Article 47(1)		
656	1. In relation to each European attestation scheme activity referred to in Article 22(1), the following fees shall be levied towards applicants within the meaning of Article 21(3) or to authorised attestation providers to contribute to covering the full costs of the activities performed by ENISA:	1. In relation to each European attestation scheme activity referred to in Article 22(1), the following fees shall be levied towards applicants within the meaning of Article 21(3) or to authorised attestation providers to contribute to covering the full costs of the activities performed by ENISA:
Article 47(1), point (a)		
657	(a) issuing authorisations following examination of the requirements laid down in Article 21(3) and (4), including conducting evaluations;	(a) issuing authorisations following examination of the requirements laid down in Article 21(3) and (4), including conducting evaluations;
Article 47(1), point (b)		
658	(b) yearly maintenance of the authorisation;	(b) yearly maintenance of the authorisation;
Article 47(1), point (c)		
659	(c) renewing authorisations for providers of European individual cybersecurity skills attestations, including conducting evaluations.	(c) renewing authorisations for providers of European individual cybersecurity skills attestations, including conducting evaluations.
Article 47(2), first subparagraph		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
660	2.In relation to certification, the following fees shall be levied on the conformity assessment bodies for the maintenance of European cybersecurity certification schemes under which European cybersecurity certificates are issued, in particular:	2.In relation to certification, the following fees shall be levied on the conformity assessment bodies for the maintenance of European cybersecurity certification schemes under which European cybersecurity certificates are issued, in particular:
Article 47(2), first subparagraph, point (a)		
661	(a) an annual fee for the participation in a European cybersecurity certification scheme;	(a) an annual fee for the ***active*** participation in a European cybersecurity certification scheme; Recital to be added: Conformity assessment bodies that have issued a European cybersecurity certificate in a given calendar year should be understood as actively participating in a European cybersecurity certification scheme for purposes of levying an annual fee for maintenance of certification in that calendar year.
Article 47(2), first subparagraph, point (b)		
662	(b) a fee for issuance of European cybersecurity certificates under European cybersecurity certification schemes.	(b) a fee for issuance of European cybersecurity certificates under European cybersecurity certification schemes.
Article 47(2), second subparagraph		
663	The fees referred to in point b) shall be levied when the conformity assessment body submits European cybersecurity certificates to ENISA for publication on their website pursuant to Article 79.	The fees referred to in point b) shall ***only*** be levied when the conformity assessment body submits European cybersecurity certificates to ENISA for publication on their website pursuant to Article 79. Sentence to be added at the end of Recital 68: "The fees for the issuance of certificates under such schemes should not be levied on the conformity assessment body where the conformity assessment body has not issued any certificates in a given year".
Article 47(3)		
664	3.In relation to testing tools referred to in Article 15(1), a fee shall be levied on any public authority or private body for their use.	3.In relation to testing tools referred to in Article ~~15(1)~~***15(1a)***, a fee shall be levied on any public authority or private body for their use.
Article 47(4)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
665	4.Fees shall be expressed and payable in euro.	4.Fees shall be expressed and payable in euro.
Article 47(5)		
666	5.The Commission shall adopt implementing acts laying down detailed rules relating to determining the fees to be levied by ENISA, specifying in particular the estimated costs attributable to each of the matters for which fees pursuant to paragraphs 1, 2 and 3 are chargeable, and the individual fee amounts chargeable, as well as the ways and conditions under which the fees should be paid. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2). The Commission shall consult ENISA when preparing those draft implementing acts.	5.The Commission shall adopt implementing acts laying down detailed rules relating to determining the fees to be levied by ENISA, specifying in particular the estimated costs attributable to each of the matters for which fees pursuant to paragraphs 1, 2 and 3 are chargeable, and the individual fee amounts chargeable, as well as the ways and conditions under which the fees should be paid. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2). The Commission shall consult ENISA when preparing those draft implementing acts.
Article 47(6), first subparagraph		
667	6.The fees determined by the implementing acts referred in paragraph 5 shall be set out in advance to be proportionate to the estimated costs of the activities performed or services delivered as determined in a cost-effective way and shall be sufficient to cover those costs. All expenditure of ENISA attributed to staff involved in activities referred to in paragraphs 1, 2 and 3 shall be reflected in the costs to cover. Fees shall be set at such a level as to avoid a deficit or a significant accumulation of surplus in ENISA's budget. Budgetary surpluses generated through fees shall be carried over to fund activities of ENISA, in particular future activities related to fees, or offset the losses incurred. If a significant positive balance in the budget, resulting from activities covered by fees, becomes recurrent, or if a significant negative balance results from the provision of the services covered by fees, the Commission shall amend the implementing acts referred to in paragraph 5 to revise the method for calculating the fees in accordance with Article 118(2).	6.The fees determined by the implementing acts referred in paragraph 5 shall be set out in advance to be proportionate to the estimated costs of the activities performed or services delivered *and be sufficient to cover those costs* as determined in a cost-effective way. *The specific interest and needs of microenterprises and small and medium-sized enterprises, including start-ups,* ~~*and*~~ shall be ~~*sufficient to cover those costs*~~*also taken into account when determining the fees*. All expenditure of ENISA attributed to staff involved in activities referred to in paragraphs 1, 2 and 3 shall be reflected in the costs to cover. Fees shall be set at such a level as to avoid a deficit or a significant accumulation of surplus in ENISA's budget. Budgetary surpluses generated through fees shall be carried over to fund activities of ENISA, in particular future activities related to fees, or offset the losses incurred. If a significant positive balance in the budget, resulting from activities covered by fees, becomes recurrent, or if a significant negative balance results from the provision of the services covered by fees, the Commission shall amend the implementing acts referred to in paragraph 5 to revise the method for calculating the fees in accordance with Article 118(2).
Article 47(6), second subparagraph		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
668	The amount of the fees for the tasks referred to in paragraph 1 shall be fixed at such a level as to ensure that the revenue in respect thereof sufficiently contributes to cover the costs of the activities related to the development and maintenance of European individual attestation schemes, the processing of applications and the delivery and renewal of authorisations and the necessary for those oversight activities by ENISA.	The amount of the fees for the tasks referred to in paragraph 1 shall be fixed at such a level as to ensure that the revenue in respect thereof sufficiently contributes to cover the costs of the activities related to the development and maintenance of European individual attestation schemes, the processing of applications and the delivery and renewal of authorisations and the necessary for those oversight activities by ENISA.
Article 47(6), third subparagraph		
669	The amount of the fees for the tasks referred to in paragraph 2 shall be fixed at such a level as to ensure that the revenue in respect thereof sufficiently contributes to cover the full costs of the activities related to maintaining the European cybersecurity certification schemes set out in Article 75.	The amount of the fees for the tasks referred to in paragraph 2 shall be fixed at such a level as to ensure that the revenue in respect thereof sufficiently contributes to cover the full costs of the activities related to maintaining the European cybersecurity certification schemes set out in Article 75.
Article 47(6), fourth subparagraph		
670	The amount of the fees for the tasks referred to in paragraph 3 shall be fixed at such a level as to ensure that the revenue in respect thereof sufficiently contributes to cover the costs of the activities related to the provision of testing tools as set out in Article 15(1).	The amount of the fees for the tasks referred to in paragraph 3 shall be fixed at such a level as to ensure that the revenue in respect thereof sufficiently contributes to cover the costs of the activities related to the provision of testing tools as set out in Article 15(1).
Article 47(7)		
671	7.ENISA shall provide a report on the fees levied and their impact on its budget as part of the procedure for the presentation of accounts laid down in Article 50.	7.ENISA shall provide a report on the fees levied and their impact on its budget as part of the procedure for the presentation of accounts laid down in Article 50.
Article 47(8)		
672	8.ENISA shall put in place a set of indicators to measure the workload, effectiveness and efficiency in relation to activities financed through fees. ENISA shall adapt its staff planning and management of resources related to fees accordingly to be able to adequately respond to such demand and to any fluctuations in revenue from fees. ENISA shall share the report with the Commission, which the Commission may use for the purpose of the evaluation referred to in Article 120(1).	8.ENISA shall put in place a set of indicators to measure the workload, effectiveness and efficiency in relation to activities financed through fees. ENISA shall adapt its staff planning and management of resources related to fees accordingly to be able to adequately respond to such demand and to any fluctuations in revenue from fees. ENISA shall share the report with the Commission, which the Commission may use for the purpose of the evaluation referred to in Article 120(1).

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 48		
673	Article 48 Implementation of ENISA's budget	Article 48 Implementation of ENISA's budget
Article 48(1)		
674	1. The Executive Director shall be responsible for the implementation of ENISA's budget and shall act as authorising officer.	1. The Executive Director shall be responsible for the implementation of ENISA's budget and shall act as authorising officer.
Article 48(2)		
675	2. The Commission's internal auditor shall exercise the same powers over ENISA as over Commission departments.	2. The Commission's internal auditor shall exercise the same powers over ENISA as over Commission departments.
Article 48(3)		
676	3. Each year, the Executive Director shall send to the budgetary authority all information relevant to the findings of evaluation procedures.	3. Each year, the Executive Director shall send to the budgetary authority all information relevant to the findings of evaluation procedures.
Article 49		
677	Article 49 Presentation of accounts and discharge	Article 49 Presentation of accounts and discharge
Article 49(1)		
678	1. ENISA's accounting officer shall send the provisional accounts for the financial year (year N) to the Commission's accounting officer and to the Court of Auditors by 1 March of the following financial year (year N + 1).	1. ENISA's accounting officer shall send the provisional accounts for the financial year (year N) to the Commission's accounting officer and to the Court of Auditors by 1 March of the following financial year (year N + 1).
Article 49(2)		
679	2. ENISA's accounting officer shall also provide the required accounting information for consolidation purposes to the Commission's accounting officer, in the manner and format required by the latter by 1 March of year N + 1.	2. ENISA's accounting officer shall also provide the required accounting information for consolidation purposes to the Commission's accounting officer, in the manner and format required by the latter by 1 March of year N + 1.
Article 49(3)		
680	3. ENISA shall send the report on the budgetary and financial management for	3. ENISA shall send the report on the budgetary and financial management for

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	year N to the European Parliament, the Council, the Commission and the Court of Auditors by 31 March of year N + 1.	year N to the European Parliament, the Council, the Commission and the Court of Auditors by 31 March of year N + 1.
Article 49(4)		
681	4. On receipt of the Court of Auditor's observations on ENISA's provisional accounts for year N, ENISA's accounting officer shall draw up ENISA's final accounts on their own responsibility. The Executive Director shall submit them to the Management Board for an opinion.	4. On receipt of the Court of Auditor's observations on ENISA's provisional accounts for year N, ENISA's accounting officer shall draw up ENISA's final accounts on their own responsibility. The Executive Director shall submit them to the Management Board for an opinion.
Article 49(5)		
682	5. The Management Board shall deliver an opinion on ENISA's final accounts for year N.	5. The Management Board shall deliver an opinion on ENISA's final accounts for year N.
Article 49(6)		
683	6. ENISA's accounting officer shall, by 1 July of year N + 1 send the final accounts for year N to the European Parliament, the Council, the Commission and the Court of Auditors, together with the Management Board's opinion.	6. ENISA's accounting officer shall, by 1 July of year N + 1 send the final accounts for year N to the European Parliament, the Council, the Commission and the Court of Auditors, together with the Management Board's opinion.
Article 49(7)		
684	7. A link to the web pages containing ENISA's final accounts shall be published in the Official Journal of the European Union by 15 November of year N + 1.	7. A link to the web pages containing ENISA's final accounts shall be published in the Official Journal of the European Union by 15 November of year N + 1.
Article 49(8)		
685	8. The Executive Director shall send to the Court of Auditors, by 30 September of year N + 1, a reply to the observations made in its annual report. The Executive Director shall also send that reply to the Management Board and to the Commission.	8. The Executive Director shall send to the Court of Auditors, by 30 September of year N + 1, a reply to the observations made in its annual report. The Executive Director shall also send that reply to the Management Board and to the Commission.
Article 49(9)		
686	9. The Executive Director shall submit to the European Parliament, at the latter's request, any information required for the smooth application of the discharge procedure for year N, in accordance with Article 267(3) of Regulation (EU,	9. The Executive Director shall submit to the European Parliament, at the latter's request, any information required for the smooth application of the discharge procedure for year N, in accordance with Article 267(3) of Regulation (EU,

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	Euratom) 2024/2509 of the European Parliament and of the Council.	Euratom) 2024/2509 of the European Parliament and of the Council.
Article 49(10)		
687	10. On a recommendation from the Council acting by qualified majority, the European Parliament shall, before 15 May of year N + 2, give a discharge to the Executive Director in respect of the implementation of the budget for year N.	10. On a recommendation from the Council acting by qualified majority, the European Parliament shall, before 15 May of year N + 2, give a discharge to the Executive Director in respect of the implementation of the budget for year N.
Article 50		
688	Article 50 Financial rules	Article 50 Financial rules
Article 50(1)		
689	1.The financial rules applicable to ENISA shall be adopted by the Management Board after consulting the Commission. They shall not depart from Delegated Regulation (EU) 2019/715 unless such a departure is specifically required for the operation of ENISA and the Commission has given its prior consent.	1.The financial rules applicable to ENISA shall be adopted by the Management Board after consulting the Commission. They shall not depart from Delegated Regulation (EU) 2019/715 unless such a departure is specifically required for the operation of ENISA and the Commission has given its prior consent.
Article 50(2)		
690	2.ENISA shall establish and implement its budget in accordance with its financial rules and Regulation (EU, Euratom) 2024/2509.	2.ENISA shall establish and implement its budget in accordance with its financial rules and Regulation (EU, Euratom) 2024/2509.
Article 51		
691	Article 51 Combating fraud	Article 51 Combating fraud
Article 51(1)		
692	1.In order to combat fraud, corruption and other unlawful activities, the provisions of Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council [1] shall apply without restriction to the activities of ENISA. _____ 1. Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11	1.In order to combat fraud, corruption and other unlawful activities, the provisions of Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council [1] shall apply without restriction to the activities of ENISA. _____ 1. Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999 (OJ L 248, 18.9.2013, p. 1, ELI: http://data.europa.eu/eli/reg/2013/883/oj).	September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999 (OJ L 248, 18.9.2013, p. 1, ELI: http://data.europa.eu/eli/reg/2013/883/oj).
Article 51(2)		
693	2.ENISA shall accede to the Interinstitutional Agreement of 25 May 1999 between the European Parliament, the Council of the European Union and the Commission of the European Communities concerning internal investigations by the European Anti-Fraud Office (OLAF)[1] within six months from [OP please insert the exact date, as referred to in Art. 127] and shall adopt the appropriate provisions applicable to its staff using the template set out in the Annex to that Agreement. _____ 1. OJ L 136, 31.5.1999, p. 15, ELI: http://data.europa.eu/eli/agree_interinstit/1999/531/oj.	2.ENISA shall accede to the Interinstitutional Agreement of 25 May 1999 between the European Parliament, the Council of the European Union and the Commission of the European Communities concerning internal investigations by the European Anti-Fraud Office (OLAF)[1] within six months from [OP please insert the exact date, as referred to in Art. 127] and shall adopt the appropriate provisions applicable to its staff using the template set out in the Annex to that Agreement. _____ 1. OJ L 136, 31.5.1999, p. 15, ELI: http://data.europa.eu/eli/agree_interinstit/1999/531/oj.
Article 51(3)		
694	3.The Court of Auditors shall have the power of audit, on the basis of documents and on-the-spot checks, over all grant beneficiaries, contractors and subcontractors who have received Union funds from ENISA.	3.The Court of Auditors shall have the power of audit, on the basis of documents and on-the-spot checks, over all grant beneficiaries, contractors and subcontractors who have received Union funds from ENISA.
Article 51(4)		
695	4.OLAF may carry out investigations, including on-the-spot checks and inspections with a view to establishing whether there has been fraud, corruption or any other illegal activity affecting the financial interests of the Union in connection with a grant or a contract funded by ENISA, in accordance with the provisions and procedures laid down in Regulation (EU, Euratom) No 883/2013 and Council Regulation (Euratom, EC) No 2185/96[1]. _____ 1. Council Regulation (Euratom, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities (OJ L 292, 15.11.1996, p. 2, ELI: http://data.europa.eu/eli/reg/1996/2185/oj).	4.OLAF may carry out investigations, including on-the-spot checks and inspections with a view to establishing whether there has been fraud, corruption or any other illegal activity affecting the financial interests of the Union in connection with a grant or a contract funded by ENISA, in accordance with the provisions and procedures laid down in Regulation (EU, Euratom) No 883/2013 and Council Regulation (Euratom, EC) No 2185/96[1]. _____ 1. Council Regulation (Euratom, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities (OJ L 292, 15.11.1996, p. 2, ELI: http://data.europa.eu/eli/reg/1996/2185/oj).

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 51(5)		
696	5.Without prejudice to paragraphs 1to 4, working agreements with third countries and international organisations, contracts, grant agreements and grant decisions of ENISA shall contain provisions expressly empowering the Court of Auditors and OLAF to conduct such audits and investigations, according to their respective competencies.	5.Without prejudice to paragraphs 1to 4, working agreements with third countries and international organisations, contracts, grant agreements and grant decisions of ENISA shall contain provisions expressly empowering the Court of Auditors and OLAF to conduct such audits and investigations, according to their respective competencies.
Article 51(6)		
697	6.In accordance with Council Regulation (EU) 2017/1939, the EPPO may investigate and prosecute fraud and other illegal activities affecting the financial interests of the Union as provided for in Directive (EU) 2017/1371 of the European Parliament and of the Council[1]. _____ 1. Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law (OJ L 198, 28.7.2017, p. 29, ELI: http://data.europa.eu/eli/dir/2017/1371/oj).	6.In accordance with Council Regulation (EU) 2017/1939, the EPPO may investigate and prosecute fraud and other illegal activities affecting the financial interests of the Union as provided for in Directive (EU) 2017/1371 of the European Parliament and of the Council[1]. _____ 1. Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law (OJ L 198, 28.7.2017, p. 29, ELI: http://data.europa.eu/eli/dir/2017/1371/oj).
Article 52		
698	Article 52 Declaration of interests	Article 52 Declaration of interests
Article 52(1)		
699	1.Members of the Management Board, the Executive Director, the Deputy Executive Director, and officials seconded by Member States on a temporary basis, shall each make a declaration of commitments and a declaration indicating the absence or presence of any direct or indirect interest which might be considered to be prejudicial to their independence. The declarations shall be accurate and complete, shall be made annually in writing, and shall be updated whenever necessary.	1.Members of the Management Board, the Executive Director, the Deputy Executive Director, and officials seconded by Member States on a temporary basis, shall each make a declaration of commitments and a declaration indicating the absence or presence of any direct or indirect interest which might be considered to be prejudicial to their independence. The declarations shall be accurate and complete, shall be made annually in writing, and shall be updated whenever necessary.
Article 52(2)		
700	2.Members of the Management Board, the Executive Director, the Deputy	2.Members of the Management Board, the Executive Director, the Deputy

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	Executive Director, external experts participating in ad hoc working groups, shall each accurately and completely declare, at the latest at the start of each meeting, any interest which might be considered to be prejudicial to their independence in relation to the items on the agenda, and shall abstain from participating in the discussion of and voting on such items.	Executive Director, external experts participating in ad hoc working groups, shall each accurately and completely declare, at the latest at the start of each meeting, any interest which might be considered to be prejudicial to their independence in relation to the items on the agenda, and shall abstain from participating in the discussion of and voting on such items.
Article 52(3)		
701	3.ENISA shall lay down, in its internal rules of operation, the practical arrangements for the rules on declarations of interest referred to in paragraphs 1 and 2.	3.ENISA shall lay down, in its internal rules of operation, the practical arrangements for the rules on declarations of interest referred to in paragraphs 1 and 2.
Article 53		
702	Article 53 Transparency	Article 53 Transparency
Article 53(1)		
703	1.ENISA shall carry out its activities with a high level of transparency and in accordance with Article 55.	1.ENISA shall carry out its activities with a high level of transparency and in accordance with Article 55.
Article 53(2)		
704	2.ENISA shall ensure that the public and any interested parties are provided with appropriate, objective, reliable and easily accessible information, in particular with regard to the results of its work. It shall also make publicly available the declarations of interest made in accordance with Article 52.	2.ENISA shall ensure that the public and any interested parties are provided with appropriate, objective, reliable and easily accessible information, in particular with regard to the results of its work. It shall also make publicly available the declarations of interest made in accordance with Article 52.
Article 53(3)		
705	3.The Management Board, acting on a proposal from the Executive Director, may authorise interested parties to observe the proceedings of some of ENISA's activities.	3.The Management Board, acting on a proposal from the Executive Director, may authorise interested parties to observe the proceedings of some of ENISA's activities.
Article 53(4)		
706	4.ENISA shall lay down, in its internal rules of operation, the practical	4.ENISA shall lay down, in its internal rules of operation, the practical

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	arrangements for implementing the transparency rules referred to in paragraphs 1 and 2.	arrangements for implementing the transparency rules referred to in paragraphs 1 and 2.
Article 54		
707	Article 54 Confidentiality within ENISA	Article 54 Confidentiality within ENISA
Article 54(1)		
708	1. Without prejudice to Article 55, ENISA shall not disclose to third parties information that it processes or receives in relation to which a reasoned request for confidential treatment has been made.	1. Without prejudice to Article 55, ENISA shall not disclose to third parties information that it processes or receives in relation to which a reasoned request for confidential treatment has been made.
Article 54(2)		
709	2. Members of the Management Board, the Executive Director, the Deputy Executive Director, the members of the ENISA Advisory Group, external experts participating in ad hoc working groups, and members of the staff of ENISA, including officials seconded by Member States on a temporary basis, shall comply with the confidentiality requirements of Article 339 TFEU, even after their duties have ceased.	2. Members of the Management Board, the Executive Director, the Deputy Executive Director, the members of the ENISA Advisory Group, external experts participating in ad hoc working groups, and members of the staff of ENISA, including officials seconded by Member States on a temporary basis, shall comply with the confidentiality requirements of Article 339 TFEU, even after their duties have ceased.
Article 54(3)		
710	3. ENISA shall lay down, in its internal rules of operation, the practical arrangements for implementing the confidentiality rules referred to in paragraphs 1 and 2.	3. ENISA shall lay down, in its internal rules of operation, the practical arrangements for implementing the confidentiality rules referred to in paragraphs 1 and 2.
Article 55		
711	Article 55 Access to documents	Article 55 Access to documents
Article 55(1)		
712	1. Regulation (EC) No 1049/2001 shall apply to documents held by ENISA.	1. Regulation (EC) No 1049/2001 shall apply to documents held by ENISA.
Article 55(2)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
713	2. The Management Board shall adopt arrangements for implementing Regulation (EC) No 1049/2001.	2. The Management Board shall adopt arrangements for implementing Regulation (EC) No 1049/2001. Decision 2019/17 of the ENISA Management Board.
Article 55(3)		
714	3. Decisions taken by ENISA pursuant to Article 8 of Regulation (EC) No 1049/2001 may be the subject of a complaint to the European Ombudsman under Article 228 TFEU or of an action before the Court of Justice of the European Union under Article 263 TFEU.	3. Decisions taken by ENISA pursuant to Article 8 of Regulation (EC) No 1049/2001 may be the subject of a complaint to the European Ombudsman under Article 228 TFEU or of an action before the Court of Justice of the European Union under Article 263 TFEU.
CHAPTER V		
715	CHAPTER V Staff and Liaison Officers	CHAPTER V Staff and Liaison Officers
Article 56		
716	Article 56 General provisions	Article 56 General provisions
Article 56(1)		
717	1. The Staff Regulations of Officials and the Conditions of Employment of Other Servants, as well as the rules adopted by agreement between the Union institutions for giving effect to the Staff Regulations of Officials and the Conditions of Employment of Other Servants shall apply to the staff of ENISA.	1. The Staff Regulations of Officials and the Conditions of Employment of Other Servants, as well as the rules adopted by agreement between the Union institutions for giving effect to the Staff Regulations of Officials and the Conditions of Employment of Other Servants shall apply to the staff of ENISA.
Article 56(2)		
718	2. The staff of ENISA, liaison officers and seconded national experts to ENISA shall undergo appropriate security clearance procedure.	2. The staff of ENISA, liaison officers and seconded national experts to ENISA shall undergo appropriate security clearance procedure.
Article 57		
719	Article 57 Privileges and immunities	Article 57 Privileges and immunities

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 57, first paragraph		
720	Protocol No 7 on the privileges and immunities of the European Union, annexed to the TFEU, shall apply to ENISA and its staff.	Protocol No 7 on the privileges and immunities of the European Union, annexed to the TFEU, shall apply to ENISA and its staff.
Article 58		
721	Article 58 Liaison officers	Article 58 Liaison officers
Article 58(1)		
722	1. Each Member State shall designate at least two liaison officers from a national competent authority designated pursuant to Article 8(1) of Directive (EU) 2022/2555 as seconded national experts to ENISA to work at its seat or its local office, in accordance with Article 59(2). The Commission may also designate a liaison officer.	1. Each Member State ~~shall~~***may*** designate ~~at least two~~***one or more*** liaison officers from a national competent authority designated pursuant to Article 8(1) of Directive (EU) 2022/2555 as seconded national experts to ENISA to work at its seat or its local office, in accordance with Article 59(2). The Commission may also designate a liaison officer.
Article 58(2)		
723	2. Liaison officers shall contribute to executing the tasks of ENISA, including by facilitating operational cooperation and exchange of information as referred to in Article 11. Liaison officers shall also support ENISA in disseminating information about its activities, findings and recommendations to relevant stakeholders across the Union. They shall also act as national contact points for questions from their Member States and relating to their Member States, either by answering those questions directly or by liaising with their national administrations.	2. Liaison officers shall contribute to executing the tasks of ENISA, including by facilitating operational cooperation and exchange of information as referred to in Article 11. Liaison officers shall also support ENISA in disseminating information about its activities, findings and recommendations to relevant stakeholders across the Union. They shall also act as national contact points for questions from their Member States and relating to their Member States, either by answering those questions directly or by liaising with their national administrations.
Article 58(3)		
724	3. Liaison officers designated by their Member States shall be entitled to request and receive all relevant information from their Member States, as provided for by this Regulation, while fully respecting the national law and the Member State's practices, in particular as regards data protection and confidentiality.	3. Liaison officers designated by their Member States shall be entitled to request and receive all relevant information from their Member States, as provided for by this Regulation, while fully respecting the national law and the Member State's practices, in particular as regards data protection and confidentiality.
Article 59		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
725	Article 59 Seconded national experts and other staff	Article 59 Seconded national experts and other staff
Article 59(1)		
726	1.ENISA may make use of seconded national experts or other staff not employed by ENISA, in any areas of its work. The Staff Regulations and the Conditions of Employment shall not apply to such staff.	1.ENISA may make use of seconded national experts or other staff not employed by ENISA, in any areas of its work. The Staff Regulations and the Conditions of Employment shall not apply to such staff.
Article 59(2)		
727	2.The Management Board shall adopt a decision laying down rules on the secondment of national experts, including liaison officers, to ENISA.	2.The Management Board shall adopt a decision laying down rules on the secondment of national experts, including liaison officers, to ENISA.
CHAPTER VI		
728	CHAPTER VI GENERAL PROVISIONS CONCERNING ENISA	CHAPTER VI GENERAL PROVISIONS CONCERNING ENISA
Article 60		
729	Article 60 Legal status of ENISA	Article 60 Legal status of ENISA
Article 60(1)		
730	1.ENISA shall be a body of the Union with legal personality.	1.ENISA shall be a body of the Union with legal personality.
Article 60(2)		
731	2.In each Member State, ENISA shall enjoy the most extensive legal capacity accorded to legal persons under that Member State's national law. It may, in particular, acquire or dispose of movable and immovable property and be a party to legal proceedings.	2.In each Member State, ENISA shall enjoy the most extensive legal capacity accorded to legal persons under that Member State's national law. It may, in particular, acquire or dispose of movable and immovable property and be a party to legal proceedings.
Article 60(3)		
732	3.ENISA shall be represented by the Executive Director.	3.ENISA shall be represented by the Executive Director.
Article 61		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
733	Article 61 Seat	Article 61 Seat
Article 61, first paragraph		
734	ENISA shall have its seat in Athens, Greece.	ENISA shall have its seat in Athens, Greece.
Article 62		
735	Article 62 Headquarters Agreement and operating conditions	Article 62 Headquarters Agreement and operating conditions
Article 62(1)		
736	1. The necessary arrangements concerning the accommodation to be provided for ENISA in the host Member State and the facilities to be made available by that Member State together with the specific rules applicable in the host Member State to the Executive Director, members of the Management Board, ENISA's staff and members of their families shall be laid down in a headquarters agreement between ENISA and the host Member State, concluded after obtaining the approval of the Management Board.	1. The necessary arrangements concerning the accommodation to be provided for ENISA in the host Member State and the facilities to be made available by that Member State together with the specific rules applicable in the host Member State to the Executive Director, members of the Management Board, ENISA's staff and members of their families shall be laid down in a headquarters agreement between ENISA and the host Member State, concluded after obtaining the approval of the Management Board.
Article 62(2)		
737	2. ENISA's host Member State shall provide the best possible conditions for ensuring the proper functioning of ENISA, taking into account the accessibility of the location, the existence of adequate education facilities for the children of staff members, appropriate access to the labour market, social security and medical care for both children and spouses of staff members.	2. ENISA's host Member State shall provide the best possible conditions for ensuring the proper functioning of ENISA, taking into account the accessibility of the location, the existence of adequate education facilities for the children of staff members, appropriate access to the labour market, social security and medical care for both children and spouses of staff members.
Article 63		
738	Article 63 Administrative control	Article 63 Administrative control
Article 63, first paragraph		
739	The operations of ENISA shall be supervised by the European Ombudsman in	The operations of ENISA shall be supervised by the European Ombudsman in

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	accordance with Article 228 TFEU.	accordance with Article 228 TFEU.
Article 64		
740	Article 64 Liability of ENISA	Article 64 Liability of ENISA
Article 64(1)		
741	1. The contractual liability of ENISA shall be governed by the law applicable to the contract in question.	1. The contractual liability of ENISA shall be governed by the law applicable to the contract in question.
Article 64(2)		
742	2. The Court of Justice of the European Union shall have jurisdiction to give judgment pursuant to any arbitration clause contained in a contract concluded by ENISA.	2. The Court of Justice of the European Union shall have jurisdiction to give judgment pursuant to any arbitration clause contained in a contract concluded by ENISA.
Article 64(3)		
743	3. In the case of non-contractual liability, ENISA shall make good any damage caused by it or its staff in the performance of their duties, in accordance with the general principles common to the laws of the Member States.	3. In the case of non-contractual liability, ENISA shall make good any damage caused by it or its staff in the performance of their duties, in accordance with the general principles common to the laws of the Member States.
Article 64(4)		
744	4. The Court of Justice of the European Union shall have jurisdiction in disputes overcompensation for damages referred to in paragraph 3.	4. The Court of Justice of the European Union shall have jurisdiction in disputes overcompensation for damages referred to in paragraph 3.
Article 64(5)		
745	5. The personal liability of ENISA's staff towards ENISA shall be governed by the provisions laid down in the Staff Regulations or Conditions of Employment applicable to them.	5. The personal liability of ENISA's staff towards ENISA shall be governed by the provisions laid down in the Staff Regulations or Conditions of Employment applicable to them.
Article 65		
746	Article 65 Language arrangements	Article 65 Language arrangements

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 65(1)		
747	1. Council Regulation No 1[1] shall apply to ENISA. The Member States and the other bodies appointed by the Member States may address ENISA and receive a reply in the official language of the institutions of the Union that they choose. _____ 1. Council Regulation No 1 determining the languages to be used by the European Economic Community (OJ 17, 6.10.1958, p. 385, ELI: http://data.europa.eu/eli/reg/1958/1(1)/oj).	1. Council Regulation No 1[1] shall apply to ENISA. The Member States and the other bodies appointed by the Member States may address ENISA and receive a reply in the official language of the institutions of the Union that they choose. _____ 1. Council Regulation No 1 determining the languages to be used by the European Economic Community (OJ 17, 6.10.1958, p. 385, ELI: http://data.europa.eu/eli/reg/1958/1(1)/oj).
Article 65(2)		
748	2. Translation and all other linguistic services required for the functioning of ENISA, other than interpretation, shall be provided by the Translation Centre for the Bodies of the European Union.	2. Translation and all other linguistic services required for the functioning of ENISA, other than interpretation, shall be provided by the Translation Centre for the Bodies of the European Union.
Article 66		
749	Article 66 Protection of personal data	Article 66 Protection of personal data
Article 66(1)		
750	1. The processing of personal data by ENISA shall be subject to Regulation (EU) 2018/1725.	1. The processing of personal data by ENISA shall be subject to Regulation (EU) 2018/1725.
Article 66(2)		
751	2. The Management Board shall adopt implementing rules as referred to in Article 45(3) of Regulation (EU) 2018/1725. The Management Board may adopt additional measures necessary for the application of Regulation (EU) 2018/1725 by ENISA.	2. The Management Board shall adopt implementing rules as referred to in Article 45(3) of Regulation (EU) 2018/1725. The Management Board may adopt additional measures necessary for the application of Regulation (EU) 2018/1725 by ENISA. Decision 2019/2.
Article 67		
752	Article 67 Security rules on the protection of sensitive non-classified information and	Article 67 Security rules on the protection of sensitive non-classified information and

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	classified information	classified information, *and the use of information sharing protocols*
Article 67, first paragraph		
753	In agreement with the Commission, ENISA shall adopt security rules applying the security principles contained in the Commission's security rules for protecting sensitive non-classified information and EUCI, as set out in Decisions (EU, Euratom) 2015/443[1] and 2015/444[2]. Those security rules shall include provisions for the exchange, processing and storage of such information. _____ 1. Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41, ELI: http://data.europa.eu/eli/dec/2015/443/oj). 2. Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53, ELI: http://data.europa.eu/eli/dec/2015/444/oj).	In agreement with the Commission, ~~*ENISA*~~*the Management Board* shall adopt security rules applying the security principles contained in the Commission's security rules for protecting sensitive non-classified information and EUCI, as set out in Decisions (EU, Euratom) 2015/443[1] and 2015/444[2]. Those security rules shall include provisions for the exchange, processing and storage of such information. _____ 1. Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41, ELI: http://data.europa.eu/eli/dec/2015/443/oj). 2. Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53, ELI: http://data.europa.eu/eli/dec/2015/444/oj).
Article 67, first paragraph a		
753a		*When sharing or exchanging information pursuant to this Regulation, ENISA shall respect relevant information sharing protocols, including the traffic light protocol.*
Article 68		
754	Article 68 Cooperation with Union entities and national authorities	Article 68 Cooperation with Union entities and national authorities
Article 68(1)		
755	1. To ensure consistency, create synergies and address issues of common concern, ENISA shall cooperate on matters related to cybersecurity with CERT-EU and relevant Union entities, including Europol, the European Cybersecurity Industrial, Technology and Research Competence Centre established pursuant to Regulation (EU) 2021/887, and the European Data Protection Board established pursuant to Article 68(1) of Regulation (EU) 2016/679.	1. To ensure consistency, create synergies and address issues of common concern, ENISA shall cooperate on matters related to cybersecurity with CERT-EU and relevant Union entities, including Europol, the European Cybersecurity Industrial, Technology and Research Competence Centre *as well as the network of national coordination centres* established pursuant to Regulation (EU) 2021/887, ~~*and*~~ the European Data Protection Board established pursuant to

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
		Article 68(1) of Regulation (EU) 2016/679 *and the European Data Protection Supervisor*.
Article 68(2)		
756	2. The cooperation referred to in paragraph 1 may be ensured by means of:	2. The cooperation referred to in paragraph 1 may be ensured by means of:
Article 68(2), point (a)		
757	(a) the exchange of know-how and best practices;	(a) the exchange of know-how and best practices;
Article 68(2), point (b)		
758	(b) the provision of advice and issuance of guidance on matters related to cybersecurity;	(b) the provision of advice and issuance of guidance on matters related to cybersecurity;
Article 68(2), point (c)		
759	(c) the establishment of practical arrangements for the execution of specific tasks, after consulting the Commission.	(c) the establishment of practical arrangements for the execution of specific tasks, after consulting the Commission *and the Management Board*.
Article 68(3)		
760	3. ENISA shall engage in a structured cooperation with CERT-EU, in particular on matters related to capacity-building, operational cooperation, and long-term strategic analyses of cyber threats.	3. ENISA shall engage in a structured cooperation with CERT-EU, in particular on matters related to capacity-building, operational cooperation, and long-term strategic analyses of cyber threats.
Article 68(4)		
761	4. ENISA shall cooperate and exchange information with relevant market surveillance and supervisory authorities designated under Union legislation in the field of cybersecurity, including Regulation (EU) 2024/2847.	4. ENISA shall cooperate and exchange information with relevant market surveillance and supervisory authorities designated under Union legislation in the field of cybersecurity, including Regulation (EU) 2024/2847.
Article 69		
762	Article 69 Cooperation with stakeholders	Article 69 Cooperation with stakeholders
Article 69(1)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
763	1. Where necessary to achieve the objectives of this Regulation, ENISA shall cooperate with relevant stakeholders, such as the cybersecurity industry, the ICT industry, SMEs, entities operating in sectors listed in Annexes I and II to Directive (EU) 2022/2555, manufacturers, importers or distributors of products with digital elements within the meaning of Regulation (EU) 2024/2847, conformity assessment bodies notified under the European cybersecurity certification framework and Regulation (EU) 2024/2847, entities operating in the area of electronic identification means, consumer groups, and academic experts in the field of cybersecurity. To that end, ENISA may establish public-private partnerships.	1. Where necessary to achieve the objectives of this Regulation, ENISA shall cooperate with relevant stakeholders, such as the cybersecurity industry, the ICT industry, SMEs, entities operating in sectors listed in Annexes I and II to Directive (EU) 2022/2555, manufacturers, importers or distributors of products with digital elements within the meaning of Regulation (EU) 2024/2847, conformity assessment bodies notified under the European cybersecurity certification framework and Regulation (EU) 2024/2847, entities operating in the area of electronic identification means, consumer groups, and academic experts in the field of cybersecurity. To that end, ENISA may establish public-private partnerships.
Article 69(1a)		
763a		*1a. The Management Board shall adopt a strategy for relations with stakeholders.*
Article 69(2)		
764	2. ENISA shall, in consultation with the Commission, support cooperation between notified conformity assessment bodies pursuant to Article 93. In particular, it may establish a group of notified conformity assessment bodies for sharing of best practices, creating synergies with other relevant Union legislation, in particular Regulation (EU) 2024/2847.	2. ENISA shall, in consultation with the Commission, support cooperation between notified conformity assessment bodies pursuant to Article 93. In particular, it may establish a group of notified conformity assessment bodies for sharing of best practices, creating synergies with other relevant Union legislation, in particular Regulation (EU) 2024/2847.
Article 70		
765	Article 70 Cooperation with third countries and international organisations	Article 70 Cooperation with third countries and international organisations
Article 70(1)		
766	1. To the extent necessary to achieve the objectives of this Regulation, ENISA may cooperate with the competent authorities of third countries or with international organisations or both, in line with the priorities of the Union. To that end, ENISA may establish working arrangements with the authorities of	1. To the extent necessary to achieve the objectives of this Regulation, ENISA may cooperate with the competent authorities of third countries or with international organisations or both, in line with the priorities of the Union. To that end, ENISA may establish working arrangements with the authorities of

	CLEAN Commission Proposal	VS.EC Council Mandate
	third countries and international organisations, subject to the prior approval of the Commission. Those working arrangements shall not create legal obligations incumbent on the Union and its Member States.	third countries and international organisations, subject to the prior approval of the Commission ***and the Management Board***. Those working arrangements shall not create legal obligations incumbent on the Union and its Member States. Alignment with Article 28(1)(q).
Article 70(2)		
767	2. The Management Board shall adopt a strategy for relations with third countries and international organisations concerning matters for which ENISA is competent and in line with the priorities referred to in paragraph 1. The Commission shall ensure that ENISA operates within its mandate and the existing institutional framework by concluding appropriate working arrangements with the Executive Director.	2. The Management Board shall adopt a strategy for relations with third countries and international organisations concerning matters for which ENISA is competent and in line with the priorities referred to in paragraph 1. The Commission shall ensure that ENISA operates within its mandate and the existing institutional framework by concluding appropriate working arrangements with the Executive Director.
Article 70(3)		
768	3. To support cooperation with third countries, in particular countries that are candidates for accession to the Union, ENISA may deliver its capacity-building expertise, in particular in the following areas:	3. To support cooperation with third countries, in particular countries that are candidates for accession to the Union, ENISA may deliver its capacity-building expertise, in particular in the following areas:
Article 70(3), point (a)		
769	(a) assessment of the level of maturity of cybersecurity capabilities and resources;	(a) assessment of the level of maturity of cybersecurity capabilities and resources;
Article 70(3), point (b)		
770	(b) growth and enhancement of the cybersecurity workforce, including by promoting the ECSF and the European individual cybersecurity skills attestation schemes, and providing learning and training activities;	(b) growth and enhancement of the cybersecurity workforce, including by promoting the ECSF and the European individual cybersecurity skills attestation schemes, and providing learning and training activities;
Article 70(3), point (c)		
771	(c) supporting the planning and execution of cybersecurity exercises.	(c) supporting the planning and execution of cybersecurity exercises ***and other cyber preparedness activities***.
Article 70(4)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
772	4.ENISA shall be open to the participation of third countries in ENISA's work that have concluded agreements with the Union to that effect. Under the relevant provisions of agreements concluded between third countries and the Union, working arrangements shall be established, subject to prior approval of the Commission, specifying in particular the nature, extent and manner in which those third countries are to participate in ENISA's work, and shall include provisions relating to participation in the initiatives undertaken by ENISA, to financial contributions and to staff. As regards staff matters, those working arrangements shall comply with the Staff Regulations and Conditions of Employment in any event.	4.ENISA shall be open to the participation of third countries in ENISA's work that have concluded agreements with the Union to that effect. Under the relevant provisions of agreements concluded between third countries and the Union, working arrangements shall be established, subject to prior approval of the Commission, specifying in particular the nature, extent and manner in which those third countries are to participate in ENISA's work, and shall include provisions relating to participation in the initiatives undertaken by ENISA, to financial contributions and to staff. As regards staff matters, those working arrangements shall comply with the Staff Regulations and Conditions of Employment in any event.
Article 70(5)		
773	5.ENISA shall regularly report to the Council and the Commission on the implementation of the working arrangements referred to in paragraphs 1 and 4.	5.ENISA shall regularly report to the Council and the Commission on the implementation of the working arrangements referred to in paragraphs 1 and 4.
TITLE III		
774	TITLE III EUROPEAN CYBERSECURITY CERTIFICATION FRAMEWORK	TITLE III EUROPEAN CYBERSECURITY CERTIFICATION FRAMEWORK
CHAPTER I		
775	CHAPTER I Objectives, Scope and Procedures	CHAPTER I Objectives, Scope and Procedures
Article 71		
776	Article 71 Objectives and scope of the European cybersecurity certification framework	Article 71 Objectives and scope of the European cybersecurity certification framework Recital (87) amended.
Article 71(1)		
777	1.The European cybersecurity certification framework shall be established with a view of creating a digital single market for ICT products, ICT services, ICT	1.The European cybersecurity certification framework shall be established with a view of creating a digital single market for ICT products, ICT services, ICT

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	processes, managed security services and entities. To that end, it shall increase the level of cybersecurity within the Union and enable a harmonised approach to European cybersecurity certification schemes as well as leverage certification to facilitate compliance with applicable Union legislation.	processes, managed security services and entities. To that end, it shall increase the level of cybersecurity within the Union and enable a harmonised approach to European cybersecurity certification schemes as well as leverage certification to facilitate compliance with applicable Union legislation.
Article 71(2)		
778	2. The European cybersecurity certification framework shall provide for a mechanism to establish European cybersecurity certification schemes and to attest the following:	2. The European cybersecurity certification framework shall provide for a mechanism to establish European cybersecurity certification schemes and to attest the following:
Article 71(2), point (a)		
779	(a) that the ICT products, ICT services and ICT processes that have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, services and processes throughout their lifecycle;	(a) that the ICT products, ICT services and ICT processes that have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity ~~or~~ ***and*** 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 lifecycle;
Article 71(2), point (b)		
780	(b) that managed security services that have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity and confidentiality of data which are accessed, processed, stored or transmitted in relation to the provision of those services, and that those services are provided continuously with the requisite competence, expertise and experience by staff with a sufficient and appropriate level of relevant technical knowledge and professional integrity;	(b) that managed security services that have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity and confidentiality of data which are accessed, processed, stored or transmitted in relation to the provision of those services, and that those services are provided continuously with the requisite competence, expertise and experience by staff with a sufficient and appropriate level of relevant technical knowledge and professional integrity;
Article 71(2), point (c)		
781	(c) that the cyber posture of an entity that has been evaluated in accordance with such schemes complies with specified cybersecurity requirements.	(c) that the cyber posture of an entity that has been evaluated in accordance with such schemes ***continuously*** complies with specified cybersecurity requirements.

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 71(3)		
782	3. European cybersecurity certification shall be voluntary, unless otherwise specified in Union or national law.	3. European cybersecurity certification shall be voluntary, unless otherwise ~~specified~~ ***specifically provided for*** in Union or national law~~.~~ Recital (87) amended.
Article 71(4)		
783	4. A European cybersecurity certificate and EU statement of conformity issued under the European cybersecurity certification framework shall be automatically recognised in all Member States.	4. A European cybersecurity certificate and EU statement of conformity issued under the European cybersecurity certification framework shall be ~~automatically~~ recognised in all Member States.
Article 72		
784	Article 72 Public information and consultation	Article 72 Public information and consultation
Article 72(1)		
785	1. At least once a year, the Commission shall organise, with the support of ENISA, a European Cybersecurity Certification Assembly, inviting ECCG members and other relevant experts from Member States, relevant experts from Union entities and relevant stakeholders to discuss strategic priorities for harmonisation in the area of cybersecurity certification.	1. At least once a year, the Commission shall organise, with the support of ENISA, a European Cybersecurity Certification Assembly, inviting ECCG members and other relevant experts from Member States, relevant experts from Union entities***, bodies established pursuant to Union law*** and relevant stakeholders to discuss strategic priorities for harmonisation in the area of cybersecurity certification. See also Recital 86.
Article 72(2)		
786	2. The Commission shall maintain and regularly update a dedicated website providing information on the following aspects:	2. The Commission shall maintain and regularly update a dedicated ***section on its*** website providing information on the following aspects: See also Recital 84.
Article 72(2), point (a)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
787	(a) European cybersecurity certification schemes requested for development pursuant to Article 73;	(a) European cybersecurity certification schemes requested for development pursuant to Article 73*, including the development plan and current status of the schemes*;
Article 72(2), point (b)		
788	(b) strategic priorities for harmonisation of ICT products, ICT services, ICT processes, managed security services, cyber posture of entities or security requirements of Union legislation, including potential areas for which a European cybersecurity certification scheme might be requested.	(b) strategic priorities for harmonisation of *certification for* ICT products, ICT services, ICT processes, managed security services, cyber posture of entities or security requirements of Union legislation, including potential areas for which a European cybersecurity certification scheme might be requested.
Article 72(2), point (ba)		
788a		*(ba) information on, and the agendas of the planned meetings of the European Cybersecurity Certification Assembly, and main conclusions of the previous meetings.* See also Recital 84.
Article 72(3)		
789	3. The Commission shall make publicly available on the website referred to in paragraph 2 of this Article the information on its request to ENISA to prepare a candidate scheme as referred to in Article 73 and its decision to accept, reject or discontinue a candidate scheme transmitted by ENISA in accordance with Article 74(7).	3. The Commission shall make publicly available on the website referred to in paragraph 2 of this Article the information on ~~its request~~*requests* to ENISA to prepare a candidate scheme as referred to in Article 73 and *information on* its decision to accept, reject*, suspend* or discontinue a candidate scheme transmitted by ENISA in accordance with Article 74(7). *The Commission shall also make publicly available on the website any subsequent changes in the scope of the request.*
Article 72(4)		
790	4. During the preparation of a candidate scheme by ENISA pursuant to Article 74, the European Parliament and the Council may request the Commission, in its capacity as chair of the ECCG, and ENISA to present relevant information on the draft candidate scheme. Upon the request of the European Parliament or the	4. During the preparation of a candidate scheme by ENISA pursuant to Article 74, the European Parliament and the Council may request the Commission, in its capacity as chair of the ECCG, and ENISA to present relevant information on the draft candidate scheme. Upon the request of the European Parliament or the

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	Council, ENISA, in agreement with the Commission and without prejudice to Article 54, may make available to the European Parliament and to the Council relevant parts of a draft candidate scheme in a manner appropriate to the confidentiality level required, and where appropriate in a restricted manner.	Council, ENISA, in agreement with the Commission and without prejudice to Article 54, may make available to the European Parliament and to the Council relevant parts of a draft candidate scheme in a manner appropriate to the confidentiality level required, and where appropriate in a restricted manner.
Article 72(5)		
791	5. The European Parliament and the Council may invite the Commission and ENISA to discuss matters concerning the implementation of European cybersecurity certification schemes for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities.	5. The European Parliament and the Council may invite the Commission and ENISA to discuss matters concerning the implementation of European cybersecurity certification schemes for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities.
Article 73		
792	Article 73 Requests for a European cybersecurity certification scheme	Article 73 Requests for a European cybersecurity certification scheme
Article 73(1)		
793	1. The Commission may request ENISA to prepare a candidate European cybersecurity certification scheme for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities.	1. The Commission may*, where applicable following a request by the ECCG pursuant to paragraph 2,* request ENISA to prepare a candidate European cybersecurity certification scheme for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities.
Article 73(2)		
794	2. In duly justified cases, the ECCG may suggest to the Commission to put forward a request referred to in paragraph 1.	2. ~~*In duly justified cases,*~~ The ECCG may ~~*suggest to*~~*request* the Commission to put forward a request referred to in paragraph 1. *The Commission shall inform the ECCG within 30 days from the submission of such request about whether it intends to put it forward. Where the Commission decides not to put forward such a request, they shall duly justify that decision.*
Article 73(3)		
795	3. The request referred to in paragraph 1 shall detail the purpose, scope and modalities of meeting relevant security objectives and elements set out in Articles 80 and 81. The request shall also specify the development plan of the candidate	3. The request referred to in paragraph 1 shall detail the purpose, scope*, development timeframe* and modalities of meeting relevant security objectives and elements set out in Articles 80 and 81. The request shall also specify the

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	European cybersecurity certification scheme and relevant technical specifications to be referenced or defined in the scheme.	development plan of the candidate European cybersecurity certification scheme and relevant technical specifications to be referenced or defined in the scheme. *The Commission shall update the request where necessary.*
Article 73(4)		
796	4. When preparing the request referred to in paragraph 1, the Commission shall duly consult ENISA and the ECCG as well as take into account the views of all relevant stakeholders and other Union entities, including, where applicable, those that are relevant under Union legislation in which a European cybersecurity certification scheme is demonstrating compliance and providing presumption of conformity.	4. When preparing the request referred to in paragraph 1, the Commission shall duly consult ENISA and the ECCG as well as take into account *existing standards and technical specifications, national cybersecurity certification schemes and* the views of all relevant stakeholders ~~*and other*~~*,* Union entities *and bodies established pursuant to Union law*, including, where applicable, those that are relevant under Union legislation ~~*in*~~ *with* which a European cybersecurity certification scheme is demonstrating compliance and providing presumption of conformity. *The Commission may also request ENISA to conduct a feasibility study to inform the request referred to in paragraph 1.* See also Recital 86.
Article 74		
797	Article 74 Preparation and adoption of European cybersecurity certification schemes	Article 74 Preparation and adoption of European cybersecurity certification schemes
Article 74(1)		
798	1. No later than 12 months after receiving a request from the Commission pursuant to Article 73, unless otherwise specified in the request, ENISA shall prepare a candidate European cybersecurity certification scheme that meets the requirements set out in Articles 80 and 81.	1. ~~*No later than 12 months after receiving a request from the Commission pursuant to Article 73, unless otherwise specified in the request,*~~ ENISA shall prepare *and transmit to the Commission* a candidate European cybersecurity certification scheme that meets the requirements set out in Articles 80 and 81 *within 12 months from the receipt of the request referred to in Article 73, unless the request specifies a different timeframe*.
Article 74(2)		
799	2. For the preparation of each candidate scheme, ENISA shall establish an ad hoc	2. For the preparation of each candidate scheme, ENISA shall*, as soon as*

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	working group in accordance with Article 32(6) for the purpose of providing ENISA with expertise advice.	*possible,* establish an ad hoc working group in accordance with Article 32(6) for the purpose of providing ENISA with expertise advice.
Article 74(3)		
800	3. When preparing the candidate scheme, ENISA shall closely cooperate with the ECCG. The ECCG shall provide ENISA with assistance and expert advice in relation to the preparation of the candidate scheme and, where applicable, supporting technical specifications.	3. When preparing the candidate scheme, ENISA shall closely cooperate with the ECCG *at all stages of development process.* . The ECCG shall provide ENISA with assistance and expert advice in relation to the preparation of the candidate scheme and, where applicable, supporting technical specifications*, including delivering opinion(s) as referred to in paragraph 5*.
Article 74(4)		
801	4. When preparing the candidate scheme, including, where applicable, supporting technical specifications, ENISA shall consult stakeholders in a timely manner by means of a formal, open, transparent and inclusive consultation process. ENISA shall also cooperate with relevant public authorities in the Member States and with relevant Union entities to gather their expert advice in relation to the preparation of the candidate scheme and, where applicable, supporting technical specifications. When transmitting the candidate scheme to the Commission pursuant to paragraph 6, ENISA shall describe the manner in which it has complied with this paragraph.	4. When preparing the candidate scheme, including, where applicable, supporting technical specifications, ENISA shall consult stakeholders in a timely manner by means of a formal, open, transparent and inclusive consultation process. ENISA shall also cooperate with relevant public authorities in the Member States and with relevant Union entities *and bodies established pursuant to Union law,* to gather their expert advice*, including with regard to existing standards, technical specifications and national cybersecurity certification schemes,* in relation to the preparation of the candidate scheme and, where applicable, supporting technical specifications. When transmitting the candidate scheme to the Commission pursuant to paragraph 6, ENISA shall describe the manner in which it has complied with this paragraph.
Article 74(5)		
802	5. Before transmitting the candidate scheme and, where applicable, supporting technical specifications, to the Commission, ENISA shall request members of the ECCG to provide written opinions on the candidate scheme. The opinions shall be provided no later than 30 days from date of the request. ENISA shall take the utmost account of the opinions of the ECCG members. The absence of such opinions shall not prevent ENISA from transmitting the candidate scheme to the Commission.	5. Before transmitting the candidate scheme and, where applicable, supporting technical specifications, to the Commission, ENISA shall request members of the ECCG to provide written opinions on the candidate scheme. The opinions shall be provided no later than ~~30~~*60* days from date of the request. ENISA shall take the utmost account of the opinions of the ECCG members~~.~~ *and the ECCG accordingly.* The absence of such opinions shall not prevent ENISA from transmitting the candidate scheme to the Commission. *The opinions of the*

	CLEAN Commission Proposal	VS.EC Council Mandate
		ECCG members shall be shared with the ECCG. See also Recital 86a on joint opinions.
Article 74(6)		
803	6. ENISA shall transmit the candidate scheme to the Commission no later than 60 days from the date of the request referred to in paragraph 5.	6. ENISA shall transmit the candidate scheme to the Commission no later than ~~60~~ *90* days from the date of the request *for opinions* referred to in paragraph 5. *ENISA shall include information of how the opinions of the members of the ECCG were considered.*
Article 74(7)		
804	7. When receiving the candidate scheme, the Commission shall evaluate whether the scheme corresponds to the request made in accordance with Article 73. Within 30 days of the date of transmission of that candidate scheme the Commission shall take one of the following actions:	7. When receiving the candidate scheme, the Commission shall evaluate whether the scheme corresponds to the request made in accordance with Article 73. Within 30 days of the date of transmission of that candidate scheme the Commission shall take one of the following actions:
Article 74(7), point (a)		
805	(a) accept the candidate scheme;	(a) accept the candidate scheme *where it fulfils the request submitted pursuant to Article 73(3)*;
Article 74(7), point (b)		
806	(b) return the candidate scheme to ENISA for revision together with a justification for this return and a deadline not exceeding 90 days, within which ENISA shall provide a revised candidate scheme;	(b) return the candidate scheme to ENISA for revision together with a justification for this return and a deadline not exceeding 90 days, within which ENISA shall provide a revised candidate scheme;
Article 74(7), point (ba)		
806a		*(ba) in duly justified cases suspend the candidate scheme by suspending the request issued pursuant to Article 73. The Commission shall inform all relevant parties, including the ECCG, accordingly;*
Article 74(7), point (c)		
807	(c) discontinue the candidate scheme.	(c) *in duly justified cases* discontinue the candidate scheme *by withdrawing the*

	CLEAN Commission Proposal	VS.EC Council Mandate
		request issued pursuant to Article 73. The Commission shall inform all relevant parties, including the ECCG, and provide the reasons therefore.
Article 74(8)		
808	8. Where the Commission returns a candidate scheme to ENISA for revision in accordance with paragraph 7, point (b), paragraphs 4, 5 and 7 shall apply accordingly.	8. Where the Commission returns a candidate scheme to ENISA for revision in accordance with paragraph 7, point (b), paragraphs 4, 5 and 7 shall apply accordingly.
Article 74(9)		
809	9. The Commission, based on the accepted candidate scheme prepared by ENISA, is empowered to adopt implementing acts providing for a European cybersecurity certification scheme for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities that meets the requirements set out in Articles 80 and 81. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 118(2).	9. The Commission, based on the accepted candidate scheme prepared by ENISA, is empowered to adopt implementing acts providing for a European cybersecurity certification scheme *that meets the requirements set out in Articles 80 and 81* for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities ~~*that meets the requirements set out in Articles 80 and 81*~~. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 118(2). To be revisited when discussing Article 118.
Article 74(9a)		
809a		*9a. The Commission shall specify the conditions for the transition from national cybersecurity certification schemes in the implementing acts referred to in paragraph 9.*
Article 74(10)		
810	10. The Commission may reference technical specifications developed by ENISA in the implementing acts referred to in paragraph 9 of this Article, in accordance with Articles 18 and 77.	10. The Commission may reference technical specifications developed by ENISA in the implementing acts referred to in paragraph 9 of this Article, in accordance with Articles 18 and 77.
Article 74(11)		
811	11. The Commission may specify the conditions for the international recognition of European cybersecurity certificates, in the implementing acts referred to in	11. The Commission may specify the conditions for the international recognition of European cybersecurity certificates, in the implementing acts referred to in

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	paragraph 9 of this Article, in accordance with Article 87.	paragraph 9 of this Article, in accordance with Article 87.
Article 75		
812	Article 75 Maintenance of a European cybersecurity certification scheme	Article 75 Maintenance of a European cybersecurity certification scheme
Article 75(1)		
813	1. Each European cybersecurity certification scheme shall establish a maintenance strategy. The maintenance strategy shall outline expectations with regard to maintenance activities, in particular those related to the standards or technical specifications referenced in the scheme and to the interaction with relevant stakeholders.	1. Each European cybersecurity certification scheme shall ~~*establish*~~*include* a maintenance strategy. The maintenance strategy shall outline expectations with regard to maintenance activities, in particular those related to the standards or technical specifications referenced in the scheme and to the interaction with relevant stakeholders.
Article 75(2)		
814	2. ENISA, in cooperation with the Commission and supported by the ECCG and its relevant maintenance sub-group, shall ensure the maintenance of European cybersecurity certification schemes, including in view of the possible review of such schemes by the Commission. ENISA shall cooperate and exchange information with relevant Union entities and groups in relation to maintenance activities.	2. ENISA, in cooperation with the Commission and ~~*supported by*~~ the ECCG ~~*and its*~~*through the* relevant *ECCG* maintenance ~~*sub-group*~~*sub-groups as referred to in Article 90(5)*, shall ensure the maintenance of European cybersecurity certification schemes, including in view of the possible review of such schemes by the Commission. ENISA shall cooperate and exchange information with *competent authorities of Member States,* relevant Union entities*, and bodies established pursuant to Union law,* ~~*and groups*~~ in relation to maintenance activities. NEW Recital – 89a) added.
Article 75(3)		
815	3. ENISA may organise the involvement of the private sector for the maintenance of a scheme in the form of an ad hoc working group in accordance with the maintenance strategy referred to in paragraph 1.	3. ENISA may organise the involvement of the private sector for the maintenance of a scheme in the form of an ad hoc working group in accordance with the maintenance strategy referred to in paragraph 1 *and to support the work of the dedicated ECCG maintenance sub-group*.
Article 75(4)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
816	4. The maintenance activities of European cybersecurity certification schemes shall include the following:	4. The maintenance activities of European cybersecurity certification schemes shall include the following:
Article 75(4), point (a)		
817	(a) the preparation, update and endorsement of technical specifications and guidelines to support the harmonised and uniform operation of the schemes;	(a) the preparation, ~~update~~ ***review*** and endorsement of technical specifications ***as referred to in Article 77*** and guidelines ***by ENISA*** to support the harmonised and uniform operation of the schemes;
Article 75(4), point (b)		
818	(b) the identification of standards or technical specifications that are relevant to the scheme;	(b) the identification of standards or technical specifications that are relevant to the scheme***, including, where appropriate, those for which development or revision should be considered from the relevant standardisation organisations***;
Article 75(4), point (c)		
819	(c) interactions and, where relevant, the establishment of liaisons, with relevant stakeholders, including European or international standardisation organisations, including for the purpose of making or receiving technical contributions;	(c) interactions and, where relevant, the establishment of liaisons, with relevant stakeholders, including European or international standardisation organisations, including for the purpose of making or receiving technical contributions;
Article 75(4), point (d)		
820	(d) the issuance of recommendations to the Commission on necessary improvements and updates to the schemes, including in view of a possible review of the schemes;	(d) the issuance of recommendations to the Commission on necessary ~~*improvements and updates to the schemes, including in view of a possible*~~ review of the schemes;
Article 75(4), point (e)		
821	(e) the exchange of information related to the practical implementation of the schemes between Member States;	(e) the exchange of information related to the practical implementation of the schemes between Member States;
Article 75(4), point (f)		
822	(f) contributions to peer review and peer assessment mechanisms and analyses of the outcome of such assessments to improve the operation of the schemes and support their possible review.	(f) contributions to ~~*peer review and*~~ peer assessment mechanisms and analyses of the outcome of such assessments to improve the operation of the schemes and support their possible review.
Article 75(5)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
823	5. The ECCG may issue an opinion on the maintenance of European cybersecurity certification schemes.	5. The ECCG may issue an opinion on the maintenance of European cybersecurity certification schemes. *The Commission and ENISA shall take due account of it.*
Article 76		
824	Article 76 Evaluation, review and withdrawal of a European cybersecurity certification scheme	Article 76 Evaluation, review and withdrawal of a European cybersecurity certification scheme
Article 76(1)		
825	1. At least every four years following the entry into application of a European cybersecurity certification scheme, ENISA shall evaluate the impact and effectiveness of that scheme, in cooperation with the relevant maintenance sub-group of the ECCG, and by taking into account the feedback received from stakeholders. ENISA shall conduct the evaluation by carrying out the market analysis in accordance with Article 8(1).	1. At least every four years following the entry into application of a European cybersecurity certification scheme, ENISA shall evaluate the impact and effectiveness of that scheme, in cooperation with the relevant maintenance sub-group of the ECCG, and by taking into account the feedback received from stakeholders. ENISA shall conduct the evaluation by carrying out the market analysis in accordance with Article 8(1).
Article 76(1a)		
825a		*1a. The Commission, on its own motion or upon request of the ECCG, may request ENISA to carry out an ad hoc assessment of a European cybersecurity certification scheme prior to the four-year evaluation cycle referred to in paragraph 1. Where such a request is duly justified by emerging risks or significant changes in the threat landscape, the Commission shall, where appropriate, request ENISA to assess whether a revision of the scheme is necessary.*
Article 76(2)		
826	2. Following the evaluation referred to in paragraph 1, the Commission may review or withdraw implementing acts providing for a European cybersecurity certification scheme pursuant to Article 74(9).	2. Following the evaluation referred to in paragraph 1 *and recommendations issued pursuant to Article 75(4)(d)*, the Commission may review or withdraw implementing acts providing for a European cybersecurity certification scheme pursuant to Article 74(9).

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 76(3)		
827	3. When reviewing or withdrawing European cybersecurity certification schemes, the Commission shall consult ENISA, the ECCG and its relevant maintenance sub-group, as well as take into account the views of relevant stakeholders and other Union entities.	3. When reviewing or withdrawing European cybersecurity certification schemes, the Commission shall consult ENISA, the ECCG and its relevant maintenance sub-group, as well as take into account the views of relevant stakeholders ~~and other~~, Union entities *and bodies established pursuant to Union law*.
Article 76(4)		
828	4. The ECCG may issue an opinion on the review or withdrawal of a European cybersecurity certification scheme. The Commission shall take due account of it when reviewing or withdrawing the European cybersecurity certification scheme.	4. The ECCG may issue an opinion on the review or withdrawal of a European cybersecurity certification scheme. The Commission shall take due account of it when reviewing or withdrawing the European cybersecurity certification scheme *and, if it does not follow the opinion, it shall duly justify its decision*. NEW Recital 90a) added.
Article 77		
829	Article 77 Technical specifications in European cybersecurity certification schemes	Article 77 Technical specifications in European cybersecurity certification schemes
Article 77(1)		
830	1. ENISA may develop technical specifications in view of a future European cybersecurity certification scheme or in support of the maintenance of a European cybersecurity certification scheme.	1. *In the absence of appropriate European or international standards, or where such standards are insufficient or at such an early stage of development that they cannot reasonably be expected to be available within the timeframe required for the certification scheme,* ENISA may develop technical specifications *as referred to in Article 18* in view of a future European cybersecurity certification scheme or in support of the maintenance of a European cybersecurity certification scheme.
Article 77(2)		
831	2. The technical specifications referred to in paragraph 1 of this Article shall be developed in a timely manner, with the support of the ECCG and its	2. The technical specifications referred to in paragraph 1 of this Article shall be developed *in accordance with Article 18,* in a timely manner, with the support of

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	maintenance sub-groups and, where applicable, the corresponding ad hoc working group as referred to in Article 75(3). For this purpose, ENISA shall also seek contributions from relevant stakeholder groups taking into account the maintenance strategy referred to in Article 75(1).	the ECCG and its maintenance sub-groups and, where applicable, ~~*the corresponding ad hoc working group as referred to in Article 75(3). For this purpose, ENISA shall also seek contributions from*~~ relevant stakeholder groups ~~*taking into account*~~ ***mentioned in*** the maintenance strategy referred to in Article 75(1) ***and (3)***. Commission to check internally on DK suggestion to refer to standardisation bodies.
Article 77(3)		
832	3. Where technical specifications are referenced in a European cybersecurity certification scheme as referred to in Article 74(10), they shall be made available on the website referred to in Article 79.	3. Where technical specifications are referenced in a European cybersecurity certification scheme as referred to in Article 74(10), they shall be made available on the website referred to in Article 79.
Article 77(4)		
833	4. In duly justified cases, in particular where the technical specifications contain information that could compromise the security of certified ICT products, ICT services, ICT processes, managed security services or cyber posture of entities, they shall be distributed only to those stakeholders concerned by the requirements of the scheme. Such technical specifications shall not be referenced in a European cybersecurity certification scheme as referred to in Article 74(10).	4. In duly justified cases, in particular where the technical specifications contain information that could compromise the security of certified ICT products, ICT services, ICT processes, managed security services or cyber posture of entities, they shall be distributed only to those ~~*stakeholders*~~***involved in the assessment*** concerned by the requirements of the scheme. Such technical specifications shall not be referenced in a European cybersecurity certification scheme as referred to in Article 74(10). See also Recital 92.
Article 78		
834	Article 78 Facilitation of compliance with Union legislation	Article 78 Facilitation of compliance with Union legislation
Article 78(1)		
835	1. Where a specific Union legal act so provides, a certificate issued under a European cybersecurity certification scheme shall demonstrate compliance and	1. Where a specific Union legal act so provides, a certificate issued under a European cybersecurity certification scheme shall demonstrate compliance and

	CLEAN Commission Proposal	VS.EC Council Mandate
	confer a presumption of conformity with corresponding requirements set out in that legal act.	confer a presumption of conformity with corresponding requirements set out in that legal act. See also Recital (105).
Article 78(2)		
836	2. Evaluation activities under a European cybersecurity certification scheme shall be consistent with the corresponding Union legal act setting out the demonstration of compliance and the presumption of conformity. Where such evaluation activities are not specified in the corresponding Union legal act, the scheme shall specify them. A conformity assessment for certification granting the presumption of conformity with requirements set out in Union legislation shall be conducted by a third-party body.	2. Evaluation activities under a European cybersecurity certification scheme shall be consistent with the corresponding Union legal act setting out the demonstration of compliance and the presumption of conformity. Where such evaluation activities are not specified in the corresponding Union legal act, the scheme shall specify them. A conformity assessment for certification granting the presumption of conformity with requirements set out in Union legislation shall be conducted by a ~~*third party body*~~ ***conformity assessment body accredited pursuant to this Regulation***.
Article 78(3)		
837	3. In the absence of harmonised Union legislation, national law may also provide that a European cybersecurity certification scheme may be used for demonstrating the compliance and establishing the presumption of conformity with specific legal requirements set out in national law.	3. In the absence of harmonised Union legislation, national law may also provide that a European cybersecurity certification scheme may be used for demonstrating the compliance and establishing the presumption of conformity with specific legal requirements set out in national law.
Article 79		
838	Article 79 Uptake of European cybersecurity certification schemes, ENISA website and publication of certificates	Article 79 Uptake of European cybersecurity certification schemes, ENISA website and publication of certificates
Article 79(1)		
839	1. ENISA shall organise activities to promote the uptake of adopted European cybersecurity certification schemes, including by maintaining the website referred to in paragraph 2 of this Article.	1. ENISA shall organise activities to promote the uptake of adopted European cybersecurity certification schemes, including by maintaining the website referred to in paragraph 2 of this Article.
Article 79(2)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
840	2. ENISA shall maintain and regularly update a dedicated website providing public information on the following:	2. ENISA shall maintain and regularly update a dedicated website providing public information on the following:
Article 79(2), point (a)		
841	(a) European cybersecurity certification schemes;	(a) European cybersecurity certification schemes*, including information on their development, adoption, maintenance and withdrawal*;
Article 79(2), point (b)		
842	(b) the fees associated with the maintenance of each European cybersecurity certification scheme;	(b) the fees associated with the maintenance of each European cybersecurity certification scheme; Linked to the discussion on Articles 46 and 47 on fees.
Article 79(2), point (c)		
843	(c) relevant ENISA technical specifications;	(c) relevant ENISA technical specifications *and other technical specifications referenced in a European cybersecurity certification scheme pursuant to Article 74(10)*; Merger points (c) and (g).
Article 79(2), point (d)		
844	(d) European cybersecurity certificates and EU statements of conformity, including information with regard to such certificates and statements which are no longer valid, or which are suspended, withdrawn or expired;	(d) European cybersecurity certificates and EU statements of conformity, including information with regard to such certificates and statements which are no longer valid, or which are suspended, withdrawn or expired;
Article 79(2), point (e)		
845	(e) relevant supplementary cybersecurity information provided in accordance with Article 84;	(e) relevant supplementary cybersecurity information provided in accordance with Article 84;
Article 79(2), point (f)		
846	(f) summaries of peer reviews pursuant to Article 89(7);	(f) summaries of peer reviews pursuant to Article 89(7);
Article 79(2), point (g)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
847	(g) technical specifications referenced in a European cybersecurity certification scheme pursuant to Article 74(10).	(g) ~~*technical specifications referenced in a European cybersecurity certification scheme pursuant to Article 74(10).*~~
Article 79(2), point (ga)		
847a		*(ga) whether and under which circumstances do the European cybersecurity certificates allow demonstration of compliance and the presumption of conformity with relevant cybersecurity requirements set out in other Union legislation.*
Article 79(3)		
848	3. Where applicable, the website referred to in paragraph 2 shall also indicate the national cybersecurity certification schemes that have been replaced by a European cybersecurity certification scheme.	3. Where applicable, the website referred to in paragraph 2 shall also indicate the national cybersecurity certification schemes that have been replaced by a European cybersecurity certification scheme.
CHAPTER II		
849	CHAPTER II Content of European Cybersecurity Certification Schemes	CHAPTER II Content of European Cybersecurity Certification Schemes
Article 80		
850	Article 80 Security objectives of European cybersecurity certification schemes	Article 80 Security objectives of European cybersecurity certification schemes
Article 80(1)		
851	1. A European cybersecurity certification scheme shall pursue, as applicable, the following security objectives:	1. A European cybersecurity certification scheme shall pursue, as applicable, the following security objectives:
Article 80(1), point (a)		
852	(a) to ensure that ICT products, ICT services, ICT processes and managed security services are secure by default and by design;	(a) to ensure that ICT products, ICT services, ICT processes and managed security services are secure by default and by design; NEW Recitals 6a) and b) added.
Article 80(1), point (b)		

	CLEAN Commission Proposal	VS.EC Council Mandate
853	(b) to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure using appropriate technical means, taking into account the entire lifecycle of the ICT products, ICT services or ICT processes;	(b) to protect ***the confidentiality of*** stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure using appropriate technical means, taking into account the entire lifecycle of the ICT products, ICT services or ICT processes ***and report detected breaches thereof***;
Article 8o(1), point (c)		
854	(c) to protect the integrity of stored, transmitted or otherwise processed, personal or other data, commands, programmes and configurations against any manipulation or modification not authorised by the user, and report on corruptions, taking into account the entire lifecycle of the ICT products, ICT services or ICT processes;	(c) to protect the ***availability, authenticity, and*** integrity of stored, transmitted or otherwise processed, personal or other data, commands, programmes and configurations against any manipulation or modification not authorised by the user, and report on corruptions, taking into account the entire lifecycle of the ICT products, ICT services or ICT processes;
Article 8o(1), point (d)		
855	(d) to ensure protection from unauthorised access by means of appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;	(d) to ensure protection from unauthorised access by means of appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;
Article 8o(1), point (e)		
856	(e) to identify and document components and vulnerabilities, including, where appropriate, by drawing up a software bill of materials covering at the very least the top-level dependencies;	(e) to identify and document components and vulnerabilities, including~~, *where appropriate,*~~ by drawing up a software bill of materials covering at the very least the top-level dependencies;
Article 8o(1), point (f)		
857	(f) to provide security-related information by recording and monitoring relevant internal activity, including access to or modification of data, services or functions, where applicable, with an opt-out mechanism for the user;	(f) to provide security-related information by recording and monitoring relevant internal activity, including access to or modification of data, services or functions, ~~*where applicable,*~~ with an opt-out mechanism for the user;
Article 8o(1), point (g)		
858	(g) to verify that ICT products, ICT services and ICT processes do not contain known exploitable vulnerabilities;	(g) to verify that ICT products, ICT services and ICT processes do not contain known exploitable vulnerabilities;
Article 8o(1), point (h)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
859	(h) to protect the availability of essential and basic functions, including after an incident, including through resilience and mitigation measures against denial-of-service attacks;	(h) to protect the availability of essential and basic functions, ~~*including*~~***also*** after an incident, including through resilience and mitigation measures against denial-of-service attacks;
Article 8o(1), point (i)		
860	(i) to minimise the negative impact on the availability of services provided by other networks and devices in the event of a physical or technical incident;	(i) to minimise the negative impact on the availability of services provided by other networks and devices in the event of a physical or technical incident;
Article 8o(1), point (j)		
861	(j) to ensure that ICT products, ICT services and ICT processes are regularly tested and their security reviewed;	(j) to ensure that ICT products, ICT services and ICT processes are regularly tested and their security reviewed;
Article 8o(1), point (k)		
862	(k) to ensure that vulnerabilities are addressed and remediated without delay, including through security updates, and that information about fixed vulnerabilities is shared and publicly disclosed, unless the risks of publication outweigh the security benefits;	(k) to ensure that vulnerabilities are addressed and remediated without delay, including through security updates, and that information about fixed vulnerabilities is shared and publicly disclosed, unless the risks of publication outweigh the security benefits;
Article 8o(1), point (l)		
863	(l) to ensure that a policy on coordinated vulnerability disclosure is in place;	(l) to ensure that a policy on coordinated vulnerability disclosure is in place;
Article 8o(1), point (m)		
864	(m) to facilitate the sharing of information about potential vulnerabilities in ICT products, ICT services and ICT processes;	(m) to facilitate the sharing of information about potential vulnerabilities in ICT products, ICT services and ICT processes;
Article 8o(1), point (n)		
865	(n) to ensure that, where security updates are available to address identified security issues, those security updates are disseminated without delay;	(n) to ensure that, where security updates are available to address identified security issues, those security updates are disseminated without delay;
Article 8o(1), point (o)		
866	(o) to ensure that the managed security services are provided with the requisite competence, expertise and experience, including that the staff tasked with	(o) to ensure that the managed security services are provided with the requisite competence, expertise and experience, including that the staff tasked with

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	providing those services have a sufficient and appropriate level of technical knowledge and competence in the specific field, sufficient and appropriate experience, and the highest degree of professional integrity;	providing those services have a 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 80(1), point (p)		
867	(p) to ensure that the ICT products, ICT services and ICT processes deployed in the provision of the managed security services are secure by design and by default and, where applicable, include the latest security updates and do not contain publicly known vulnerabilities;	(p) to ensure that the ICT products, ICT services and ICT processes deployed in the provision of the managed security services are secure by design and by default and, where applicable, include the latest security updates and do not contain ~~*publicly*~~ known ***exploitable*** vulnerabilities;
Article 80(1), point (q)		
868	(q) to ensure that the certified entity has appropriate internal procedures in place to ensure that services are provided at a sufficient and appropriate level of quality;	(q) to ensure that the ~~*certified*~~ entity has appropriate ~~*internal procedures*~~ ***security controls*** in place to ensure that services are provided at a sufficient and appropriate level of quality;
Article 80(1), point (r)		
869	(r) to ensure that the certified entity is able to identify, protect against, detect, respond to, and recover from incidents;	(r) to ensure that the ~~*certified*~~ entity is able to identify, protect against, detect, respond to, and recover from incidents;
Article 80(1), point (s)		
870	(s) to ensure that the certified entity is able to manage the risks posed to the security of network and information systems used by the entity for its operations or for the provision of its services, and to prevent or minimise the impact of incidents on recipients of its services and on other services;	(s) to ensure that the ~~*certified*~~ entity is able to manage the risks posed to the security of network and information systems used by the entity for its operations or for the provision of its services, and to prevent or minimise the impact of incidents on recipients of its services and on other services;
Article 80(1), point (t)		
871	(t) to ensure that the certified entity is able to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, that it has in place the full range of ICT-related capabilities needed to address the security of the network and information systems that are used by the entity, and that support the continued provision of services and their quality, including	(t) to ensure that the ~~*certified*~~ entity is able to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, that it has in place the full range of ICT-related capabilities needed to address the security of the network and information systems that are used by the entity, and that support the continued provision of services and their quality, including

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	throughout disruptions;	throughout disruptions;
Article 80(1), point (u)		
872	(u) to ensure that the certified entity is able to implement and maintain an information security management system;	(u) to ensure that the ~~certified~~ entity is able to implement and maintain an information security management system;
Article 80(1), point (v)		
873	(v) to resist any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, the network and information system used by the entity, and to ensure the continued provision of services and their quality, including throughout disruptions;	(v) *to ensure the ability* to resist*, at a given level of confidence,* any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, the network and information system used by the entity, and to ensure the continued provision of services and their quality, including throughout disruptions;
Article 80(1), point (w)		
874	(w) to ensure that the entity is able to ensure the security of processing of personal data.	(w) to ensure that the entity is able to ensure the security of processing of personal data.
Article 80(2)		
875	2. The Commission is empowered to adopt delegated acts in accordance with Article 119 to amend paragraph 1 of this Article by adding or modifying security objectives in order to ensure that they reflect the latest technological development and new related threats as well as adoption of new Union legislation setting out the demonstration of compliance and the presumption of conformity through European cybersecurity certification with relevant cybersecurity requirements of that legislation.	2. The Commission is empowered to adopt delegated acts in accordance with Article 119 to amend paragraph 1 of this Article by adding or modifying security objectives in order to ensure that they reflect the latest technological development and new related threats as well as adoption of new Union legislation setting out the demonstration of compliance and the presumption of conformity through European cybersecurity certification with relevant cybersecurity requirements of that legislation. *When preparing delegated acts updating security objectives, the Commission shall consult ENISA.* See also Article 119(4), which provides for the consultation of Member States' experts.
Article 80(3)		
876	3. A European cybersecurity certification scheme addressing products with	3. ~~*A European cybersecurity certification scheme addressing products with*~~

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	digital elements as defined in Article 3, point (1), of Regulation (EU) 2024/2847 shall be designed in alignment with the essential cybersecurity requirements set out in Annex I that Regulation and take into account available harmonised standards.	~~*digital elements as defined in Article 3, point (1), of Regulation (EU) 2024/2847 shall be designed in alignment with the essential cybersecurity requirements set out in Annex I that Regulation and take into account available harmonised standards.*~~ See also Recital 95.
Article 81		
877	Article 81 Elements of European cybersecurity certification schemes	Article 81 Elements of European cybersecurity certification schemes
Article 81(1)		
878	1. A European cybersecurity certification scheme shall include at least the following:	1. A European cybersecurity certification scheme shall include at least the following:
Article 81(1), point (a)		
879	(a) the subject matter and scope of the certification scheme, including the type or categories of ICT products, ICT services, ICT processes or managed security services, or the entity's assets, services and functions covered in scope of certification;	(a) the subject matter and scope of the certification scheme, including the type or categories of ICT products, ICT services, ICT processes or managed security services, or the entity's assets, services and functions covered in scope of certification;
Article 81(1), point (b)		
880	(b) a clear description of the purpose of the scheme and, where applicable and the identification of Union legislation setting out requirements for which the European cybersecurity certificates demonstrate compliance and confer a presumption of conformity;	(b) a clear description of the purpose of the scheme and, where applicable and the identification of Union legislation setting out requirements for which the European cybersecurity certificates demonstrate compliance and confer a presumption of conformity;
Article 81(1), point (c)		
881	(c) the maintenance strategy specifying the approach to maintenance activities set out in Article 75;	(c) the maintenance strategy specifying the approach to maintenance activities set out in Article 75;
Article 81(1), point (d)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
882	(d) the specific cybersecurity requirements, evaluation criteria and methods to be used for evaluation of ICT products, ICT services, ICT processes, managed security services or cyber posture of entities, and references to the international, European or national standards applied in the evaluation of ICT products, ICT services, ICT processes, managed security services or cyber posture of entities or, where such standards are not available or appropriate, to technical specifications drawn up by ENISA pursuant to Article 77 or, if such specifications are not available, to other technical specifications;	(d) the specific cybersecurity requirements, evaluation criteria and methods to be used for evaluation of ICT products, ICT services, ICT processes, managed security services or cyber posture of entities, and references to the international, European or national standards applied in the evaluation of ICT products, ICT services, ICT processes, managed security services or cyber posture of entities or, where such standards are not available or appropriate, to technical specifications drawn up by ENISA pursuant to Article 77 or, if such specifications are not available, to other technical specifications;
Article 81(1), point (e)		
883	(e) the maximum period of validity of European cybersecurity certificates issued under the scheme.	(e) the maximum period of validity of European cybersecurity certificates issued under the scheme.
Article 81(2)		
884	2. A European cybersecurity certification scheme shall include at least rules and conditions concerning the following:	2. A European cybersecurity certification scheme shall include at least rules and conditions concerning the following:
Article 81(2), point (a)		
885	(a) the monitoring of compliance of ICT products, ICT services, ICT processes, managed security services or cyber posture of entities with the requirements of the European cybersecurity certificates or the EU statements of conformity, including the mechanisms to demonstrate continued compliance with the specified cybersecurity requirements;	(a) the monitoring of compliance of ICT products, ICT services, ICT processes, managed security services or cyber posture of entities with the requirements of the European cybersecurity certificates or the EU statements of conformity, including the mechanisms to demonstrate continued compliance with the specified cybersecurity requirements;
Article 81(2), point (b)		
886	(b) the issuing, confirming, withdrawing and renewing of the European cybersecurity certificates, the extension or reduction of the scope of certification and the recertification;	(b) the issuing, confirming, withdrawing and renewing of the European cybersecurity certificates, the extension or reduction of the scope of certification and the recertification;
Article 81(2), point (c)		
887	(c) the consequences for ICT products, ICT services, ICT processes, managed security services or entities that have been certified or for which an EU statement	(c) the consequences for ICT products, ICT services, ICT processes, managed security services or entities that have been certified or for which an EU statement

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	of conformity has been issued, but which do not comply with the requirements of the scheme;	of conformity has been issued, but which do not comply with the requirements of the scheme;
Article 81(2), point (d)		
888	(d) how previously undetected cybersecurity vulnerabilities in ICT products, ICT services and ICT processes are to be reported and dealt with;	(d) how previously undetected cybersecurity vulnerabilities in ICT products, ICT services and ICT processes are to be reported and dealt with;
Article 81(2), point (e)		
889	(e) the content and the format of the European cybersecurity certificates and the EU statements of conformity to be issued;	(e) the content and the format of the European cybersecurity certificates and the EU statements of conformity to be issued;
Article 81(2), point (f)		
890	(f) the period of 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 or by the entity the cyber posture of which is subject to certification;	(f) the period of 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 or by the entity the cyber posture of which is subject to certification;
Article 81(2), point (g)		
891	(g) any peer assessment mechanisms established under the scheme for authorities or bodies issuing European cybersecurity certificates pursuant to Article 85(4), which shall be without prejudice to the peer review provided for in Article 90;	(g) any peer assessment mechanisms established under the scheme for authorities or bodies issuing European cybersecurity certificates pursuant to Article ~~85(4)~~ *85(3), point (ba)*, which shall be without prejudice to the peer review provided for in Article ~~90~~ *89*;
Article 81(2), point (h)		
892	(h) the confidentiality of information and data obtained by all parties in carrying out tasks and activities related to the implementation of the provisions set out in this Title;	(h) *measures for protection of* the confidentiality of information and data obtained by all parties in carrying out tasks and activities related to the implementation of the provisions set out in this Title;
Article 81(2), point (i)		
893	(i) the format and procedures to be followed by manufacturers or providers of ICT products, ICT services or ICT processes in supplying and updating the	(i) the format and procedures to be followed by manufacturers or providers of ICT products, ICT services or ICT processes in supplying and updating the

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	supplementary cybersecurity information in accordance with Article 84; and	supplementary cybersecurity information in accordance with Article 84; and
Article 81(2), point (j)		
894	(j) the continuity of certification activities during extraordinary crisis situations, that are unavoidable and hinder the possibility to apply the certification scheme's rules.	(j) *the modalities for ensuring* the continuity of certification activities during extraordinary crisis situations, that are unavoidable and hinder the possibility to apply the certification scheme's rules.
Article 81(2), point (ja)		
894a		*(ja) the information which is necessary for certification and which an applicant is to provide or otherwise make available to the conformity assessment bodies;*
Article 81(3)		
895	3. A European cybersecurity certification scheme shall, where appropriate, also include the following:	3. A European cybersecurity certification scheme shall, where appropriate, also include the following:
Article 81(3), point (a)		
896	(a) one or more assurance levels and corresponding evaluation levels;	(a) one or more assurance levels and corresponding evaluation levels;
Article 81(3), point (b)		
897	(b) protection profiles to specify the security requirements that are applicable to a given category of ICT products, ICT services, ICT processes or managed security services;	(b) *one or more* protection profiles ~~*to specify the security requirements that are applicable to a given category of ICT products, ICT services, ICT processes or managed security services;*~~*;* Definition added in Article 2(27a).
Article 81(3), point (c)		
898	(c) extension profiles to set out additional security requirements, including, where applicable, security requirements set out in national provisions transposing Union law;	(c) *one or more* extension profiles ~~*to set out additional security requirements, including, where applicable, security requirements set out in national provisions transposing Union law*~~; Definition added in Article 2(27b).
Article 81(3), point (d)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
899	(d) clarification on which conformity assessment activities, including calibration, testing, certification and inspection, for assurance level 'high', or for the purpose of demonstrating compliance and granting presumption of conformity, are permitted outside the European Economic Area (EEA);	(d) clarification on which conformity assessment activities, including ***evaluation,*** calibration, testing, certification and inspection, for assurance level 'high', or for the purpose of demonstrating compliance and granting presumption of conformity, are permitted outside the European Economic Area (EEA) ***and under what conditions***;
Article 81(3), point (e)		
900	(e) the identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products, ICT services, ICT processes, managed security services or cyber posture of entities;	(e) the identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products, ICT services, ICT processes, managed security services or cyber posture of entities;
Article 81(3), point (ea)		
900a		***(ea) information on the transition from national cybersecurity certification schemes to the European cybersecurity certification scheme;***
Article 81(3), point (f)		
901	(f) additional or specific requirements to which conformity assessment bodies are subject in order to guarantee their technical competence to evaluate the cybersecurity requirements;	(f) additional or specific requirements to which conformity assessment bodies are subject in order to guarantee their technical competence to evaluate the cybersecurity requirements;
Article 81(3), point (g)		
902	(g) the information which is necessary for certification and which an applicant is to provide or otherwise make available to the conformity assessment bodies;	(g) ~~*the information which is necessary for certification and which an applicant is to provide or otherwise make available to the conformity assessment bodies;*~~
Article 81(3), point (h)		
903	(h) marks or labels and the conditions under which such marks or labels may be used;	(h) marks or labels and the conditions under which such marks or labels may be used;
Article 81(3), point (i)		
904	(i) conditions for the international recognition of European cybersecurity certificates in accordance with Article 87.	(i) conditions for the international recognition of European cybersecurity certificates in accordance with Article 87.
Article 81(4)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
905	4. The specified requirements of the European cybersecurity certification scheme shall be consistent with the requirements of Union legislation.	4. The specified requirements of the European cybersecurity certification scheme shall be consistent with the requirements of Union legislation.
Article 81(5)		
906	5. The Commission is empowered to adopt implementing acts laying down common principles and model provisions for elements set out in paragraphs 1, 2 and 3 across European cybersecurity certification schemes. Where appropriate and available, a European cybersecurity certification scheme may include references to those principles and model provisions.	5. The Commission is empowered to adopt implementing acts laying down common principles and model provisions for elements set out in paragraphs 1, 2 and 3 across European cybersecurity certification schemes. Where appropriate and available, a European cybersecurity certification scheme may include references to those principles and model provisions.
Article 81(6)		
907	6. The implementing acts referred to in paragraph 5 shall be adopted in accordance with the examination procedure referred to in Article 118(2). When developing or revising the common principles and model provisions for the elements of European cybersecurity certification schemes, the Commission shall consult ENISA and take into account, as appropriate, views expressed by the ECCG, relevant stakeholders and other relevant bodies.	6. The implementing acts referred to in paragraph 5 shall be adopted in accordance with the examination procedure referred to in Article 118(2). When developing or revising the common principles and model provisions for the elements of European cybersecurity certification schemes, the Commission shall consult ENISA and ***the ECCG and*** take into account, as appropriate, views expressed by ~~***the ECCG,***~~ relevant stakeholders and other relevant bodies.
Article 82		
908	Article 82 Assurance and evaluation levels of European cybersecurity certification schemes	Article 82 Assurance and evaluation levels of European cybersecurity certification schemes
Article 82(1)		
909	1. A European cybersecurity certification scheme may specify one or more of the following assurance levels for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities: "basic", "substantial" or "high". Those assurance levels shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service, ICT process, managed security service, or with the nature of entities, the cyber posture of which is subject to certification, and their operational environment, 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, managed security services or cyber posture of entities: "basic", "substantial" or "high". Those assurance levels shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service, ICT process, managed security service, or with the nature of entities, the cyber posture of which is subject to certification, and their operational environment, in terms of the probability and impact of an incident.

PUBLIC

	CLEAN	Commission Proposal	VS.EC	Council Mandate
Article 82(2)				
910		2. European cybersecurity certificates shall refer to any assurance level specified in the European cybersecurity certification scheme under which those certificates are issued. EU statements of conformity shall refer to the assurance level "basic".		2. European cybersecurity certificates shall refer to any assurance level specified in the European cybersecurity certification scheme under which those certificates are issued. EU statements of conformity shall refer to the assurance level "basic".
Article 82(3)				
911		3. The security requirements corresponding to each assurance level shall be provided in the relevant European cybersecurity certification scheme, including the corresponding security controls and the corresponding evaluation that the ICT product, ICT service, ICT process, managed security service or cyber posture of entity is to undergo.		3. The security requirements corresponding to each assurance level shall be provided in the relevant European cybersecurity certification scheme, including the corresponding security controls and the corresponding evaluation that the ICT product, ICT service, ICT process, managed security service or cyber posture of entity is to undergo.
Article 82(4)				
912		4. The European cybersecurity certificate or the EU statement of conformity shall refer to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of or to prevent cybersecurity incidents.		4. The European cybersecurity certificate or the EU statement of conformity shall refer to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk ***and impact*** of ~~*or to prevent*~~ cybersecurity incidents ***or to prevent them***.
Article 82(5)				
913		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, managed security services or cyber posture of entities for which that certificate or that EU statement of conformity is issued meet the corresponding security requirements, including security controls, 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 the technical documentation. Where such a review is not appropriate, substitute evaluation activities with equivalent effect shall be undertaken.		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, managed security services or cyber posture of entities for which that certificate or that EU statement of conformity is issued meet the corresponding security requirements, including security controls, 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 the technical documentation. Where such a review is not appropriate, substitute evaluation activities with equivalent effect shall be undertaken.
Article 82(6)				

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
914	6. A European cybersecurity certificate that refers to assurance level "substantial" shall provide assurance that the ICT products, ICT services, ICT processes, managed security services or cyber posture of entities for which that certificate is issued meet the corresponding security requirements, including security controls, and that they have been evaluated at a level intended to minimise known risks of incidents and cyberattacks and the risk of cyberattacks carried out by actors with limited skills and resources. The evaluation activities to be undertaken shall include at least a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the ICT products, ICT services, ICT processes, managed security services or entities correctly implement the necessary security controls. 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, managed security services or cyber posture of entities for which that certificate is issued meet the corresponding security requirements, including security controls, and that they have been evaluated at a level intended to minimise known risks of incidents and cyberattacks and the risk of cyberattacks carried out by actors with limited skills and resources. The evaluation activities to be undertaken shall include at least a review to demonstrate the absence of ~~*publicly*~~ known ***exploitable*** vulnerabilities and testing to demonstrate that the ICT products, ICT services, ICT processes, managed security services or entities correctly implement the necessary security controls. Where any such evaluation activities are not appropriate, substitute evaluation activities with equivalent effect shall be undertaken.
Article 82(7), first subparagraph		
915	7. A European cybersecurity certificate that refers to assurance level "high" shall provide assurance that the ICT products, ICT services, ICT processes, managed security services or cyber posture of entities for which that certificate is issued meet the corresponding security requirements, including security controls, and that they have been evaluated at a level intended to minimise the risk of incidents and 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:	7. A European cybersecurity certificate that refers to assurance level "high" shall provide assurance that the ICT products, ICT services, ICT processes, managed security services or cyber posture of entities for which that certificate is issued meet the corresponding security requirements, including security controls, and that they have been evaluated at a level intended to minimise the risk of incidents and 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:
Article 82(7), first subparagraph, point (a)		
916	(a) a review to demonstrate the absence of publicly known vulnerabilities;	(a) a review to demonstrate the absence of ~~*publicly*~~ known ***exploitable*** vulnerabilities;
Article 82(7), first subparagraph, point (b)		
917	(b) testing to demonstrate that the ICT products, ICT services, ICT processes, managed security services or entities correctly implement the necessary security	(b) testing to demonstrate that the ICT products, ICT services, ICT processes, managed security services or entities correctly implement the necessary security

	CLEAN Commission Proposal	VS.EC Council Mandate
	controls at the state of the art;	controls at the state of the art;
Article 82(7), first subparagraph, point (c)		
918	(c) an assessment of the resistance of the ICT products, ICT services, ICT processes, managed security services or entities to skilled attackers, using, where relevant, penetration testing.	(c) an assessment of the resistance of the ICT products, ICT services, ICT processes, managed security services or entities to skilled attackers, using, where relevant, penetration testing.
Article 82(7), second subparagraph		
919	Where any such evaluation activities are not appropriate, substitute activities with equivalent effect shall be undertaken. Any conformity assessment activities, including calibration, testing, certification and inspection, for assurance level 'high' shall be undertaken in the European Economic Area, unless otherwise provided for in a European cybersecurity certification scheme.	Where any such evaluation activities are not appropriate, substitute activities with equivalent effect shall be undertaken. Any conformity assessment activities, including ***evaluation,*** calibration, testing, certification and inspection, for assurance level 'high' shall be undertaken in the European Economic Area, unless otherwise provided for in a European cybersecurity certification scheme.
Article 82(8)		
920	8. Where a European cybersecurity certification scheme is designed to demonstrate compliance and grant presumption of conformity with a specific Union legal act, a European cybersecurity certificate shall provide assurance that the certified ICT products, ICT services, ICT processes, managed security services or cyber posture of entities meet the corresponding cybersecurity requirements of that legal act. Any conformity assessment activities, including calibration, testing, certification and inspection, for the purpose of presumption of conformity shall be undertaken in the European Economic Area, unless otherwise provided for in a European cybersecurity certification scheme.	8. Where a European cybersecurity certification scheme is designed to demonstrate compliance and grant presumption of conformity with a specific Union legal act, a European cybersecurity certificate shall provide assurance that the certified ICT products, ICT services, ICT processes, managed security services or cyber posture of entities meet the corresponding cybersecurity requirements of that legal act. Any conformity assessment activities, including ***evaluation,*** calibration, testing, certification and inspection, for the purpose of presumption of conformity shall be undertaken in the European Economic Area, unless otherwise provided for in a European cybersecurity certification scheme.
Article 82(9)		
921	9. A European cybersecurity certification scheme may specify several evaluation levels for a given assurance level. Each of the evaluation levels shall correspond to one of the assurance levels.	9. A European cybersecurity certification scheme may specify several evaluation levels for a given assurance level. Each of the evaluation levels shall correspond to one of the assurance levels.
Article 83		
922	Article 83	Article 83

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	Conformity self-assessment	Conformity self-assessment
Article 83(1)		
923	1. A European cybersecurity certification scheme may allow for conformity self-assessment under the sole responsibility of the manufacturer or provider of ICT products, ICT services, ICT processes, managed security services or the entity the cyber posture of which is subject to certification. Conformity self-assessment shall be permitted only in relation to ICT products, ICT services, ICT processes, managed security services or cyber posture of entities that present a low risk corresponding to assurance level "basic".	1. A European cybersecurity certification scheme may allow for conformity self-assessment under the sole responsibility of the manufacturer or provider of ICT products, ICT services, ICT processes, managed security services or the entity the cyber posture of which is subject to certification. Conformity self-assessment shall be permitted only in relation to ICT products, ICT services, ICT processes, managed security services or cyber posture of entities that present a low risk corresponding to assurance level "basic".
Article 83(2)		
924	2. The manufacturer or provider of ICT products, ICT services, ICT processes, managed security services or the entity the cyber posture of which is subject to certification may issue an EU statement of conformity stating that the fulfilment of the requirements set out in the European cybersecurity certification scheme has been demonstrated. By issuing such a statement, that manufacturer or provider or entity assumes responsibility for the compliance of the ICT product, ICT service, ICT process, managed security service or cyber posture with the requirements set out in that scheme.	2. The manufacturer or provider of ICT products, ICT services, ICT processes, managed security services or the entity the cyber posture of which is subject to certification may issue an EU statement of conformity stating that the fulfilment of the requirements set out in the European cybersecurity certification scheme has been demonstrated. By issuing such a statement, that manufacturer or provider or entity assumes responsibility for the compliance of the ICT product, ICT service, ICT process, managed security service or cyber posture with the requirements set out in that scheme.
Article 83(3)		
925	3. The manufacturer or provider of ICT products, ICT services, ICT processes, managed security services or the entity the cyber posture of which is subject to certification shall make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity of the ICT products, ICT services, ICT processes, managed security services or cyber posture with the European cybersecurity certification scheme available to the national cybersecurity certification authority designated pursuant to Article 89 for the period provided for in that scheme. A copy of the EU statement of conformity shall be submitted without undue delay to the national cybersecurity	3. The manufacturer or provider of ICT products, ICT services, ICT processes, managed security services or the entity the cyber posture of which is subject to certification shall make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity of the ICT products, ICT services, ICT processes, managed security services or cyber posture with the European cybersecurity certification scheme available *in electronic form* to the national cybersecurity certification authority designated pursuant to Article ~~89~~*88* for the period provided for in that scheme. A copy of the EU statement of conformity shall be submitted without undue delay to the

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	certification authority and to ENISA.	national cybersecurity certification authority and to ENISA.
Article 84		
926	Article 84 Supplementary cybersecurity information for certified ICT products, ICT services and ICT processes	Article 84 Supplementary cybersecurity information for certified ICT products, ICT services and ICT processes
Article 84(1)		
927	1. The manufacturer or provider of ICT products, ICT services or ICT processes for which an EU statement of conformity or European cybersecurity certificate has been issued shall make available to the user the following supplementary cybersecurity information:	1. The manufacturer or provider of ICT products, ICT services or ICT processes for which an EU statement of conformity or European cybersecurity certificate has been issued shall make available to the user the following supplementary cybersecurity information:
Article 84(1), point (a)		
928	(a) the intended purpose of the relevant ICT product, ICT service or ICT process, including the security environment provided by the manufacturer or provider;	(a) the intended purpose of the relevant ICT product, ICT service or ICT process, including the security environment provided by the manufacturer or provider;
Article 84(1), point (b)		
929	(b) guidance and recommendations to assist users with the secure configuration, installation, deployment, operation and maintenance of the ICT products or ICT services;	(b) guidance and recommendations to assist users with the secure configuration, installation, deployment, operation ~~and~~, maintenance ***and disposal*** of the ICT products or ICT services;
Article 84(1), point (c)		
930	(c) the type of technical security support offered by the manufacturer or provider and the end date of the support period during which users can expect vulnerabilities to be handled and to receive security updates;	(c) the type of technical security support offered by the manufacturer or provider and the end date of the support period during which users can expect vulnerabilities to be handled and to receive security updates;
Article 84(1), point (d)		
931	(d) if the manufacturer or provider decides to make available a software bill of materials to the user, information on where that can be accessed.	(d) if the manufacturer or provider decides to make available a software bill of materials to the user, information on where that can be accessed.
Article 84(2)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
932	2. The manufacturer or provider of ICT products, ICT services or ICT processes for which an EU statement of conformity or European cybersecurity certificate has been issued shall make publicly available the following supplementary cybersecurity information:	2. The manufacturer or provider of ICT products, ICT services or ICT processes for which an EU statement of conformity or European cybersecurity certificate has been issued shall make publicly available the following supplementary cybersecurity information:
Article 84(2), point (a)		
933	(a) the single point of contact where information about vulnerabilities can be reported and received, and where the manufacturer's policy on coordinated vulnerability disclosure can be found;	(a) the single point of contact where information about vulnerabilities can be reported and received, and where the manufacturer's policy on coordinated vulnerability disclosure can be found;
Article 84(2), point (b)		
934	(b) information about fixed vulnerabilities, including a description of the vulnerabilities, including information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity, and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch.	(b) information about fixed vulnerabilities, including a description of the vulnerabilities, including information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity, and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch.
Article 84(3)		
935	3. The information referred to in paragraphs 1 and 2 shall be available in electronic form and shall remain available and be updated as necessary during the validity and at least for a period of five years after the expiry or withdrawal of the relevant European cybersecurity certificate or EU statement of conformity.	3. The information referred to in paragraphs 1 and 2 shall be available in electronic form and shall remain available and be updated as necessary during the validity and at least for a period of five years after the expiry or withdrawal of the relevant European cybersecurity certificate or EU statement of conformity.
Article 84(4)		
936	4. The obligations set out in paragraphs 1 and 2 shall not apply where the security of the relevant ICT product, ICT service or ICT process might be compromised if the information is made publicly available.	4. The obligations set out in paragraphs 1 and 2 shall not apply where the security of the relevant ICT product, ICT service or ICT process might be compromised if the information is made publicly available.
CHAPTER III		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
937	CHAPTER III Governance for the European Cybersecurity Certification Framework	CHAPTER III Governance for the European Cybersecurity Certification Framework
Section 1		
938	Section 1 General rules and management of European cybersecurity certification schemes	Section 1 General rules and management of European cybersecurity certification schemes
Article 85		
939	Article 85 Issuance of European cybersecurity certificates	Article 85 Issuance of European cybersecurity certificates
Article 85(1)		
940	1.ICT products, ICT services, ICT processes, managed security services or cyber posture of entities that have been certified under a European cybersecurity certification scheme shall be presumed to comply with the requirements of such scheme.	1.ICT products, ICT services, ICT processes, managed security services or cyber posture of entities that have been certified under a European cybersecurity certification scheme shall be presumed to comply with the requirements of such scheme.
Article 85(2)		
941	2.The conformity assessment bodies referred to in Article 91 shall issue European cybersecurity certificates on the basis of criteria included in the European cybersecurity certification scheme adopted pursuant to Article 74.	2.The conformity assessment bodies referred to in Article 91 shall issue European cybersecurity certificates on the basis of criteria included in the European cybersecurity certification scheme adopted pursuant to Article 74.
Article 85(3)		
942	3.By way of derogation from paragraph 2, a European cybersecurity certification scheme may provide that European cybersecurity certificates resulting from that scheme are to be issued only by one of the following public bodies:	3.By way of derogation from paragraph 2, *where* a European cybersecurity certification scheme ~~*may provide that*~~ *establishes assurance level 'high' or where a scheme so provides, the* European cybersecurity certificates resulting from that scheme *and* are to be issued only by one of the following ~~*public*~~ bodies:
Article 85(3), point (a)		
943	(a) a national cybersecurity certification authority referred to in Article 88 that is accredited as a conformity assessment body pursuant to Article 91(1);	(a) a national cybersecurity certification authority referred to in Article 88 that is accredited as a conformity assessment body pursuant to Article 91(1);
Article 85(3), point (b)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
944	(b) a public body that is accredited as a conformity assessment body pursuant to Article 91(1).	(b) a public body that is accredited as a conformity assessment body pursuant to Article 91(1).
Article 85(3), point (ba)		
944a		*(ba)a private body on the basis of a prior approval or a general delegation model.*
Article 85(4)		
945	4. Where a European cybersecurity certification scheme adopted pursuant to Article 74 establishes assurance level 'high' or where such scheme specifies otherwise, the European cybersecurity certificate under that scheme is to be issued only by a national cybersecurity certification authority as referred to in Article 88 that is accredited as a conformity assessment body pursuant to Article 91(1) or, in the following cases:	4. ~~*Where a European cybersecurity certification scheme adopted pursuant to Article 74 establishes assurance level 'high' or where such scheme specifies otherwise, the European cybersecurity certificate under that scheme is to be issued only by a national cybersecurity certification authority as referred to in Article 88 that is accredited as a conformity assessment body pursuant to Article 91(1) or, in the following cases:*~~
Article 85(4), point (a)		
946	(a) by a conformity assessment body on the basis of a prior approval model; or	(a) ~~*by a conformity assessment body on the basis of a prior approval model; or*~~
Article 85(4), point (b)		
947	(b) by a conformity assessment body on the basis of a general delegation model.	(b) ~~*by a conformity assessment body on the basis of a general delegation model.*~~
Article 85(5)		
948	5. The Commission is empowered to adopt implementing acts specifying procedures for prior approval or general delegation models referred to in paragraph 4 of this Article. In the preparation process for those implementing acts, the Commission shall consult the ECCG. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2).	5. The Commission is empowered to adopt implementing acts specifying procedures for prior approval or general delegation models referred to in paragraph ~~*4*~~*3, point (ba),* of this Article*, including the allocation of separated responsibilities between the national cybersecurity certification authority and the conformity assessment body, and the procedural steps applicable to each model*. In the preparation process for those implementing acts, the Commission shall consult the ECCG. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2).
Article 85(6)		
949	6. The natural or legal person who submits ICT products, ICT services, ICT	6. The natural or legal person who submits ICT products, ICT services, ICT

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	processes or managed security services for certification, or the entity which applies for certification of its cyber posture, shall make available all information necessary to conduct the certification to the national cybersecurity certification authority designated pursuant to Article 89, where that authority is the body issuing the European cybersecurity certificate, or to the conformity assessment body referred to in Article 91.	processes or managed security services for certification, or the entity which applies for certification of its cyber posture, shall make available all information necessary to conduct the certification to the national cybersecurity certification authority designated pursuant to Article 89, where that authority is the body issuing the European cybersecurity certificate, or to the conformity assessment body referred to in Article 91.
Article 85(7)		
950	7. Conformity assessment bodies and, where applicable, national cybersecurity certification authorities shall inform ENISA without undue delay about their decisions that affect the status of European cybersecurity certificates and EU statements of conformity in accordance with Article 94.	7. Conformity assessment bodies and, where applicable, national cybersecurity certification authorities shall inform ENISA without undue delay about their decisions that affect the status of European cybersecurity certificates and EU statements of conformity in ~~accordance with~~ *view of facilitating the performance of its task under* Article ~~94~~ *79*.
Article 85(8)		
951	8. The holder of a European cybersecurity certificate shall inform the conformity assessment body and, where applicable, national cybersecurity certification authority, referred to in paragraph 7, of any subsequently detected vulnerabilities or nonconformities concerning the certified ICT product, ICT service, ICT process, managed security service or cyber posture of entity that have a likely impact on its conformity with the certificate. That body shall forward that information without undue delay to the national cybersecurity certification authority concerned and assess the impact on the certificate in line with the scheme's conditions as referred to in Article 81(2), point (d).	8. The holder of a European cybersecurity certificate shall inform the conformity assessment body and, where applicable, national cybersecurity certification authority, referred to in paragraph 7, of any subsequently detected vulnerabilities or nonconformities concerning the certified ICT product, ICT service, ICT process, managed security service or cyber posture of entity that have a likely impact on its conformity with the certificate. That body shall forward that information without undue delay to the national cybersecurity certification authority concerned and assess the impact on the certificate in line with the scheme's conditions as referred to in Article 81(2), point (d).
Article 85(9)		
952	9. For their certified ICT products, ICT services, ICT processes or managed security services identified, for their entirety or parts thereof, as key assets pursuant to Article 102, the holders of a European cybersecurity certificate shall not use, install or otherwise integrate ICT components or components that include ICT components from high-risk suppliers in certified ICT products,	9. For their certified ICT products, ICT services, ICT processes or managed security services identified, for their entirety or parts thereof, as key assets pursuant to Article 102, the holders of a European cybersecurity certificate shall not use, install or otherwise integrate ICT components or components that include ICT components from high-risk suppliers in certified ICT products,

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	ICT services, ICT processes or managed security services.	ICT services, ICT processes or managed security services.
Article 85(10)		
953	10. A European cybersecurity certificate shall be issued for the period provided for in the European cybersecurity certification scheme and may be renewed, provided that the relevant requirements continue to be met.	10. A European cybersecurity certificate shall be issued for the period provided for in the European cybersecurity certification scheme and may be renewed, provided that the relevant requirements continue to be met *in accordance with the conditions set out in scheme*.
Article 85(11)		
954	11. The Commission shall cooperate with Member States to ensure the application of provisions related to the issuance of European cybersecurity certificates also in a view application of Article 100(4), point (b). The conformity assessment body and, where relevant, the national cybersecurity certification authority shall provide the Commission, on request and without undue delay, with all information relating to the issuance of the relevant European cybersecurity certificates or EU statements of conformity.	11. The Commission shall cooperate with Member States to ensure the *harmonized* application of provisions related to the *rejections of applications for and* issuance of European cybersecurity certificates also in ~~a~~view *of the* application of Article 100(4), point (b). The conformity assessment body and, where relevant, the national cybersecurity certification authority shall provide the Commission, on request and without undue delay, with all information relating to the *rejections of applications and* issuance of the relevant European cybersecurity certificates or EU statements of conformity.
Article 86		
955	Article 86 National cybersecurity certification schemes and certificates	Article 86 National cybersecurity certification schemes and certificates
Article 86(1)		
956	1.National cybersecurity certification schemes, and the related procedures for the ICT products, ICT services, ICT processes, managed security services and cyber posture of entities that are covered by the subject matter and scope of a European cybersecurity certification scheme shall cease to produce effects from the date established in the implementing act adopted pursuant to Article 74(9). National cybersecurity certification schemes and the related procedures for the ICT products, ICT services, ICT processes, managed security services and cyber posture of entities that are not covered by the subject matter and scope of a	1.National cybersecurity certification schemes, and the related procedures for the ICT products, ICT services, ICT processes, managed security services and cyber posture of entities that are covered by the subject matter and scope of a European cybersecurity certification scheme shall cease to produce effects from the date established in the implementing act adopted pursuant to Article 74(9). National cybersecurity certification schemes and the related procedures for the ICT products, ICT services, ICT processes, managed security services and cyber posture of entities that are not covered by the subject matter and scope of a

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	European cybersecurity certification scheme may continue to exist.	European cybersecurity certification scheme may continue to exist.
Article 86(2)		
957	2. Member States shall not introduce new national cybersecurity certification schemes or related procedures for the ICT products, ICT services, ICT processes, managed security services and cyber posture of entities already covered by the subject matter and scope of a European cybersecurity certification scheme.	2. Member States shall not introduce new national cybersecurity certification schemes or related procedures for the ICT products, ICT services, ICT processes, managed security services and cyber posture of entities already covered by the subject matter and scope of a European cybersecurity certification scheme.
Article 86(3)		
958	3. Existing certificates that were issued under national cybersecurity certification schemes and are covered by the subject matter and scope of a European cybersecurity certification scheme shall remain valid until their expiry date.	3. Existing certificates that were issued under national cybersecurity certification schemes and are covered by the subject matter and scope of a European cybersecurity certification scheme shall remain valid until their expiry date. *The relevant body who issued the certificate may take any action necessary to their maintenance but shall not extend the expiry date.*
Article 86(4)		
959	4. Member States shall notify the Commission and the ECCG before adopting new national cybersecurity certification schemes for ICT products, ICT services, ICT processes, managed security services and cyber posture of entities.	4. Member States shall notify the Commission and the ECCG before adopting new national cybersecurity certification schemes for ICT products, ICT services, ICT processes, managed security services and cyber posture of entities.
Article 86(5)		
960	5. The Commission may suggest to a Member State to withdraw a national cybersecurity certification scheme for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities, where the development of a European cybersecurity certification scheme covering such products, services, processes or cyber posture has already been requested in accordance with Article 73, taking into account the development plan of such scheme.	5. The Commission may suggest to a Member State to withdraw a national cybersecurity certification scheme for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities, where the development of a European cybersecurity certification scheme covering such products, services, processes or cyber posture has already been requested in accordance with Article 73, taking into account the development plan of such scheme. See also Recital 115.

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 87		
961	Article 87 International recognition of European cybersecurity certificates	Article 87 International recognition of ~~*European*~~ cybersecurity certificates
Article 87(1)		
962	1. Third country certificates of ICT products, ICT services, ICT processes, managed security services and cyber posture of entities may be recognised, by means of an implementing act or through the conclusion of an agreement between the Union and the third country in question or an international organisation, as equivalent to European cybersecurity certificates if the requirements of the relevant third country scheme or international organisation scheme are considered equivalent to those in European cybersecurity certification schemes. The Commission is empowered to adopt such implementing acts. The implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2).	1. Third country *or international organisation* certificates of ICT products, ICT services, ICT processes, managed security services and cyber posture of entities may be recognised, by means of an implementing act or through the conclusion of an agreement between the Union and the third country in question or an international organisation, as equivalent to European cybersecurity certificates if the requirements of the relevant third country scheme or international organisation scheme are considered equivalent to those in European cybersecurity certification schemes. The Commission is empowered to adopt such implementing acts. The implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2).
Article 87(2)		
963	2. The implementing acts and the agreements referred to in paragraph 1 shall be based on the conditions for international recognition of European cybersecurity certificates set out in accordance with Article 74(11).	2. The implementing acts and the agreements referred to in paragraph 1 shall be based on the conditions for international recognition of European cybersecurity certificates set out in accordance with Article 74(11). *When preparing those implementing acts, the Commission shall take due account of the views of the ECCG.*
Article 87(3)		
964	3. Agreements on the recognition of third country certificates or the international organisation certificates referred to in paragraph 1 shall only be concluded if they also recognize European cybersecurity certificates as equivalent to the third country certificates.	3. Agreements on the recognition of third country certificates or the international organisation certificates referred to in paragraph 1 shall only be concluded if they also recognize European cybersecurity certificates as equivalent to ~~*the*~~ third country *or international organisation* certificates.
Article 88		
965	Article 88	Article 88

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	National cybersecurity certification authorities	National cybersecurity certification authorities
Article 88(1)		
966	1. Each Member State shall designate one or more national cybersecurity certification authorities in its territory or, with the agreement of another Member State, one or more national cybersecurity certification authorities in that other Member State to be responsible for the supervisory tasks in the designating Member State.	1. Each Member State shall designate one or more national cybersecurity certification authorities in its territory or, with the agreement of another Member State, one or more national cybersecurity certification authorities in that other Member State to be responsible for the supervisory tasks in the designating Member State.
Article 88(2)		
967	2. Each Member State shall inform the Commission of the identity of the designated national cybersecurity certification authorities. Where a Member State designates more than one authority, it shall also inform the Commission about the tasks assigned to each of those authorities.	2. Each Member State shall inform the Commission of the identity of the designated national cybersecurity certification authorities. Where a Member State designates more than one authority, it shall also inform the Commission about the tasks assigned to each of those authorities.
Article 88(3)		
968	3. Each national cybersecurity certification authority shall be independent of the entities it supervises with regard to its organisation, funding decisions, legal structure and decision-making.	3. Each national cybersecurity certification authority shall be independent of the entities it supervises with regard to its organisation, funding decisions, legal structure and decision-making.
Article 88(4)		
969	4. The activities of the national cybersecurity certification authorities that relate to the issuance of European cybersecurity certificates under this Regulation shall be strictly separated from their supervisory activities set out in this Article and in Article 85(4), points (a) and (b), and that those activities are carried out independently from each other.	4. The activities of the national cybersecurity certification authorities that relate to the issuance of European cybersecurity certificates under this Regulation shall be strictly separated from their supervisory activities set out in this Article and in Article ~~85(4)~~ *85(3)*, points (a) and ~~(b), and that those activities are~~ *(ba) and* carried out independently from each other.
Article 88(5)		
970	5. Member States shall ensure that national cybersecurity certification authorities have adequate resources to exercise their powers and to carry out their tasks in an effective and efficient manner.	5. Member States shall ensure that national cybersecurity certification authorities ~~have adequate resources to exercise their powers and to~~ carry out their tasks in an effective and efficient manner *and have adequate resources, including staffing, expertise and stable financial means proportionate to the scope of the*

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
		tasks assigned under this Article.
Article 88(6)		
971	6. National cybersecurity certification authorities shall have the following tasks:	6. National cybersecurity certification authorities shall have the following tasks:
Article 88(6), point (a)		
972	(a) participate in the ECCG pursuant to Article 90(2);	(a) participate in the ECCG pursuant to Article 90(2);
Article 88(6), point (b)		
973	(b) supervise and enforce rules included in European cybersecurity certification schemes pursuant to Article 81(2), point (a), to ensure the compliance of ICT products, ICT services, ICT processes, managed security services and cyber posture of entities with the requirements of the European cybersecurity certificates that have been issued in their respective territories, in cooperation with relevant market surveillance or supervisory authorities, including, competent authorities under Directive (EU) 2022/2555 of the European Parliament and of the Council[1] or Regulation (EU) 2024/2847; _____ 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, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).	(b) supervise and enforce rules included in European cybersecurity certification schemes pursuant to Article 81(2), point (a), to ensure the compliance of ICT products, ICT services, ICT processes, managed security services and cyber posture of entities with the requirements of the European cybersecurity certificates that have been issued in their respective territories, in cooperation with relevant market surveillance or supervisory authorities, including, competent authorities under Directive (EU) 2022/2555 of the European Parliament and of the Council[1] or Regulation (EU) 2024/2847; _____ 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, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).
Article 88(6), point (c)		
974	(c) monitor, in cooperation with relevant market surveillance authorities, compliance with and enforce the obligations of the manufacturers or providers of ICT products, ICT services, ICT processes, managed security services or entities the cyber posture of which is certified set out in this Regulation that are established in their respective territories and that carry out conformity self-assessment in the corresponding European cybersecurity certification scheme;	(c) monitor, in cooperation with relevant market surveillance *authorities or other supervisory* authorities, compliance with and enforce the obligations of the manufacturers or providers of ICT products, ICT services, ICT processes, managed security services or entities the cyber posture of which is certified, set out in this Regulation that are established in their respective territories and that carry out conformity self-assessment in the corresponding European cybersecurity certification scheme;

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 88(6), point (d)		
975	(d) without prejudice to Article 91(3), actively assist and support the national accreditation bodies or other relevant authorities in the monitoring and supervision of the activities of conformity assessment bodies, for the purposes of this Regulation;	(d) without prejudice to Article 91(3), actively assist and support the national accreditation bodies or other relevant authorities in the monitoring and supervision of the activities of conformity assessment bodies, for the purposes of this Regulation;
Article 88(6), point (e)		
976	(e) cooperate with the Commission where the competence of a conformity assessment body is challenged pursuant to Article 94;	(e) cooperate with the Commission where the competence of a conformity assessment body is challenged pursuant to Article 94;
Article 88(6), point (f)		
977	(f) monitor and supervise the activities of the public bodies referred to in Article 85(3);	(f) monitor and supervise the activities of the public bodies referred to in Article 85(3)*, point (b)*;
Article 88(6), point (g)		
978	(g) where applicable, authorise conformity assessment bodies in accordance with Article 93, monitor compliance with and enforce the obligations of conformity assessment bodies with the additional or specific requirements set out in European cybersecurity certification schemes pursuant to Article 81(3), point (f), and restrict, suspend or withdraw existing authorisation where conformity assessment bodies do not meet the requirements of this Regulation;	(g) where applicable, authorise conformity assessment bodies in accordance with Article 93, monitor compliance with and enforce the obligations of conformity assessment bodies with the additional or specific requirements set out in European cybersecurity certification schemes pursuant to Article 81(3), point (f), and restrict, suspend or withdraw existing authorisation where conformity assessment bodies do not meet the requirements of this Regulation;
Article 88(6), point (h)		
979	(h) handle complaints by natural or legal persons in relation to European cybersecurity certificates issued by national cybersecurity certification authorities or to European cybersecurity certificates issued by conformity assessment bodies in accordance with Article 85(4) or in relation to EU statements of conformity issued under Article 83, investigate the subject matter of such complaints to the extent appropriate, and inform the complainant of the progress and the outcome of the investigation within a reasonable period;	(h) handle complaints by natural or legal persons in relation to European cybersecurity certificates issued by national cybersecurity certification authorities or to European cybersecurity certificates issued by conformity assessment bodies in accordance with Article ~~85(4)~~*85(3), point (ba),* or in relation to EU statements of conformity issued under Article 83, investigate the subject matter of such complaints to the extent appropriate, and inform the complainant of the progress and the outcome of the investigation within a reasonable period;
Article 88(6), point (i)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
980	(i) provide an annual report on its main activities to the Commission, ENISA and the ECCG by 31 March [year of entry into force + 12 months] each year, and make these reports available to the peer review team where the national cybersecurity certification authority is subject to peer review in accordance with Article 89;	(i) provide an annual report on its main activities to the Commission, ENISA and the ECCG by 31 March ***each year, from*** [year of entry into force + 12 months] ~~*each year*~~, and make these reports available to the peer review team where the national cybersecurity certification authority is subject to peer review in accordance with Article 89;
Article 88(6), point (j)		
981	(j) cooperate with other national cybersecurity certification authorities, market surveillance authorities or other public authorities, including by sharing information on the possible non-compliance of ICT products, ICT services, ICT processes, managed security services and cyber posture of entities with the requirements of this Regulation or with the requirements of specific European cybersecurity certification schemes;	(j) cooperate with other national cybersecurity certification authorities, market surveillance authorities or other public authorities, including by sharing ***necessary*** information on the possible non-compliance of ICT products, ICT services, ICT processes, managed security services and cyber posture of entities with the requirements of this Regulation or with the requirements of specific European cybersecurity certification schemes;
Article 88(6), point (k)		
982	(k) monitor relevant developments in the field of cybersecurity certification.	(k) monitor relevant developments in the field of cybersecurity certification.
Article 88(7)		
983	7.Each national cybersecurity certification authority shall have at least the following powers:	7.Each national cybersecurity certification authority shall have at least the following powers:
Article 88(7), point (a)		
984	(a) to request conformity assessment bodies, European cybersecurity certificates' holders and issuers of EU statements of conformity to provide any information it requires for the performance of its tasks;	(a) to request conformity assessment bodies, European cybersecurity certificates' holders and issuers of EU statements of conformity to provide any information it requires for the performance of its tasks;
Article 88(7), point (b)		
985	(b) to carry out investigations, in the form of audits, of conformity assessment bodies, European cybersecurity certificates' holders and issuers of EU statements of conformity, for the purpose of verifying their compliance with the requirements set out in this Title;	(b) to carry out investigations, in the form of audits, of conformity assessment bodies, European cybersecurity certificates' holders and issuers of EU statements of conformity, for the purpose of verifying their compliance with the requirements set out in this Title;
Article 88(7), point (c)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
986	(c) to take appropriate measures, in accordance with national law, to ensure that conformity assessment bodies, European cybersecurity certificates' holders and issuers of EU statements of conformity comply with this Regulation or with a European cybersecurity certification scheme;	(c) to take appropriate measures, in accordance with national law, to ensure that conformity assessment bodies, European cybersecurity certificates' holders and issuers of EU statements of conformity comply with this Regulation or with a European cybersecurity certification scheme;
Article 88(7), point (d)		
987	(d) to obtain access to the premises of any conformity assessment bodies or holders of European cybersecurity certificates, for the purpose of carrying out investigations in accordance with Union legislation or national procedural law;	(d) to obtain access to the premises of any conformity assessment bodies or holders of European cybersecurity certificates, for the purpose of carrying out investigations in accordance with Union legislation or national procedural law;
Article 88(7), point (e)		
988	(e) to withdraw, in accordance with national law, European cybersecurity certificates issued by national cybersecurity certification authorities or by conformity assessment bodies in accordance with Article 85(4), where such certificates do not comply with this Regulation or with a European cybersecurity certification scheme;	(e) to withdraw, in accordance with national law, European cybersecurity certificates issued by national cybersecurity certification authorities or by conformity assessment bodies in accordance with Article ~~85(4)~~ *85(3), point (ba)*, where such certificates do not comply with this Regulation or with a European cybersecurity certification scheme;
Article 88(7), point (f)		
989	(f) to impose penalties in accordance with national law, as provided for in Article 97, and to require the immediate cessation of infringements of the obligations set out in this Regulation.	(f) to impose penalties in accordance with national law, as provided for in Article 97, and to require the immediate cessation of infringements of the obligations set out in this Regulation.
Article 88(8)		
990	8. 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, managed security services and the cyber posture of entities.	8. 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, managed security services and the cyber posture of entities.
Article 88(9)		
991	9. By [entry into force + 6 months], ENISA shall develop a template for the report referred to in paragraph 6, point (i), of this Article, in cooperation with the	9. By [entry into force + 6 months], ENISA shall develop a template for the report referred to in paragraph 6, point (i), of this Article, in cooperation with the

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	Commission and the ECCG.	Commission and the ECCG.
Article 89		
992	Article 89 Peer review	Article 89 Peer review
Article 89(1)		
993	1.National cybersecurity certification authorities shall be subject to peer review.	1.National cybersecurity certification authorities shall be subject to peer review.
Article 89(2)		
994	2.Peer review shall be carried out on the basis of sound and transparent evaluation criteria and procedures, in particular concerning structural, human resource and process requirements, confidentiality and complaints.	2.Peer review shall be carried out on the basis of sound and transparent evaluation criteria and procedures, in particular concerning structural, human resource and process requirements, confidentiality and complaints.
Article 89(3)		
995	3.Peer review shall assess:	3.Peer review shall assess:
Article 89(3), point (a)		
996	(a) where applicable, whether the activities of the national cybersecurity certification authorities that relate to the issuance of European cybersecurity certificates referred to in this Regulation are strictly separated from their supervisory activities set out in Article 88 and whether those activities are carried out independently from each other;	(a) where applicable, whether the activities of the national cybersecurity certification authorities that relate to the issuance of European cybersecurity certificates referred to in this Regulation are strictly separated from their supervisory activities set out in Article 88 and whether those activities are carried out independently from each other;
Article 89(3), point (b)		
997	(b) the procedures for supervising and enforcing the rules for monitoring the compliance of ICT products, ICT services, ICT processes, managed security services and cyber posture of entities with European cybersecurity certificates pursuant to Article 88(7), point (a);	(b) the procedures for supervising and enforcing the rules for monitoring the compliance of ICT products, ICT services, ICT processes, managed security services and cyber posture of entities with European cybersecurity certificates pursuant to Article 88(7), point (a);
Article 89(3), point (c)		
998	(c) the procedures for monitoring and enforcing the obligations of manufacturers	(c) the procedures for monitoring and enforcing the obligations of manufacturers

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	or providers of ICT products, ICT services, ICT processes or managed security services or entities the cyber posture of which is certified, pursuant to Article 88(7), point (b);	or providers of ICT products, ICT services, ICT processes or managed security services or entities the cyber posture of which is certified, pursuant to Article 88(7), point (b);
Article 89(3), point (d)		
999	(d) the procedures for monitoring, authorising and supervising the activities of the conformity assessment bodies.	(d) the procedures for monitoring, authorising and supervising the activities of the conformity assessment bodies.
Article 89(3), point (da)		
999a		*(da)the procedures for prior approval or general delegation.*
Article 89(4)		
1000	4.Peer review shall be carried out at least once every five years by at least two national cybersecurity certification authorities of other Member States and by the Commission. ENISA shall also participate in the peer review as observer. The peer review team shall draw up the final report and the summary of the peer review.	4.Peer review shall be carried out ~~*at least*~~ once every five years by at least two national cybersecurity certification authorities of other Member States and by the Commission*. Additional peer reviews within this period may be carried out on voluntary basis*. ENISA shall also participate in the peer review as observer. The peer review team shall draw up the final report and the summary of the peer review.
Article 89(5)		
1001	5.ENISA shall support the organisation of the peer review mechanism and the peer reviews, including by developing relevant guidance documents and templates, in cooperation with the Commission and the ECCG.	5.ENISA shall support the organisation of the peer review mechanism and the peer reviews, including by developing relevant guidance documents and templates, in cooperation with the Commission and the ECCG.
Article 89(6)		
1002	6.The Commission is empowered to adopt implementing acts establishing a plan for peer review which covers a period of at least five years, laying down the criteria concerning the composition of the peer review team, the methodology to be used in peer review, and the schedule, the frequency and other tasks related to peer review. In the preparation of those implementing acts, the Commission shall consult the ECCG and ENISA. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2).	6.The Commission is empowered to adopt implementing acts establishing a plan for peer review which covers a period of at least five years, laying down the criteria concerning the composition of the peer review team, the methodology to be used in peer review, and the schedule, the frequency and other tasks related to peer review. In the preparation of those implementing acts, the Commission shall consult the ECCG and ENISA. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2).

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Article 89(7)		
1003	7. The final report, including possible guidelines or recommendations, and the summary of the peer review shall be examined by the ECCG, which shall endorse the summary for publication on the website referred to in Article 79(2).	7. The final report, including possible guidelines or recommendations, and the summary of the peer review shall be examined by the ECCG, which ~~*shall*~~ ***may*** endorse the summary for publication on the website referred to in Article 79(2). ***The summary shall not include any sensitive information about the relevant peer review.***
Article 90		
1004	Article 90 European Cybersecurity Certification Group	Article 90 European Cybersecurity Certification Group
Article 90(1)		
1005	1. The European Cybersecurity Certification Group (the 'ECCG') shall be established.	1. The European Cybersecurity Certification Group (the 'ECCG') shall be established.
Article 90(2)		
1006	2. The ECCG shall be composed of representatives of national cybersecurity certification authorities or representatives of other relevant national authorities. A member of the ECCG shall not represent more than two Member States.	2. The ECCG shall be composed of representatives of national cybersecurity certification authorities or representatives of other relevant national authorities. A member of the ECCG shall not represent more than two Member States. ***Stakeholders and relevant third parties may be invited by the ECCG to attend meetings and to participate in its work.***
Article 90(2a)		
1006a		***2a. The ECCG shall meet on a regular basis. Where appropriate, the ECCG may also engage in joint meetings with other relevant Union-level groups to address cross-cutting issues.***
Article 90(3)		
1007	3. The ECCG shall have the following tasks:	3. The ECCG shall have the following tasks:
Article 90(3), point (a)		
1008	(a) to advise and assist the Commission in its work to ensure the consistent	(a) to advise and assist the Commission in its work to ensure the consistent

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	implementation and application the rules set out in this Title, cybersecurity certification policy issues, and the coordination of policy approaches;	implementation and application ***of*** the rules set out in this Title, cybersecurity certification policy issues, and the coordination of policy approaches;
Article 90(3), point (b)		
1009	(b) to advise and assist the Commission in the preparation of requests for European cybersecurity certification schemes pursuant to Article 73;	(b) to advise and assist the Commission in the preparation of requests for European cybersecurity certification schemes pursuant to Article 73;
Article 90(3), point (c)		
1010	(c) to assist, advise and cooperate with ENISA in relation to the preparation of a candidate scheme pursuant to Article 74 and technical specifications pursuant to Article 77;	(c) to assist, advise and cooperate with ENISA in relation to the preparation of a candidate scheme pursuant to Article 74 and technical specifications pursuant to Article 77;
Article 90(3), point (d)		
1011	(d) to assist, advise and cooperate with ENISA and the Commission in relation to the maintenance activities pursuant to Article 75;	(d) to assist, advise and cooperate with ENISA and the Commission in relation to the maintenance activities pursuant to Article 75;
Article 90(3), point (e)		
1012	(e) to assist, advise and cooperate with the Commission in relation to the review or withdrawal of existing European cybersecurity certifications schemes pursuant to Article 76;	(e) to assist, advise and cooperate with the Commission in relation to the review or withdrawal of existing European cybersecurity certifications schemes pursuant to Article 76;
Article 90(3), point (f)		
1013	(f) to suggest that a request is submitted to the Commission with regard to the preparation of a candidate European cybersecurity certification scheme pursuant to Article 73(2);	(f) to ~~*suggest that a*~~ request ~~*is submitted to*~~ the Commission ***to put forward a request to ENISA*** with regard to the preparation of a candidate European cybersecurity certification scheme pursuant to Article 73(2);
Article 90(3), point (g)		
1014	(g) to adopt opinions addressed to the Commission relating to the maintenance, review and withdrawal of existing European cybersecurity certifications schemes;	(g) to adopt opinions addressed to the Commission relating to the maintenance, review and withdrawal of existing European cybersecurity certifications schemes;
Article 90(3), point (h)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
1015	(h) to examine relevant developments in the field of cybersecurity certification, including at national level pursuant to Article 86, and to exchange information and good practices on cybersecurity certification schemes;	(h) to examine relevant developments in the field of cybersecurity certification, including at national level pursuant to Article 86, and to exchange information and good practices on cybersecurity certification schemes;
Article 90(3), point (i)		
1016	(i) to facilitate the cooperation between national cybersecurity certification authorities under the rules set out in this Title through capacity-building and exchange of information, in particular relating to issues concerning cybersecurity certification;	(i) to facilitate the cooperation between national cybersecurity certification authorities under the rules set out in this Title through capacity-building and exchange of information, in particular relating to issues concerning cybersecurity certification;
Article 90(3), point (j)		
1017	(j) to support the implementation of the peer review mechanism pursuant to Article 89 and of peer assessment mechanisms in accordance with the rules established in a European cybersecurity certification scheme pursuant to Article 81(2), point (g);	(j) to support the implementation of the peer review mechanism pursuant to Article 89 and of peer assessment mechanisms in accordance with the rules established in a European cybersecurity certification scheme pursuant to Article 81(2), point (g);
Article 90(3), point (k)		
1018	(k) to facilitate the alignment of European cybersecurity certification schemes with internationally recognised standards, including as part of the maintenance of existing European cybersecurity certification schemes and, where appropriate, to make recommendations to ENISA to engage with relevant European or international standardisation organisations to address insufficiencies or gaps in available European or internationally recognised standards.	(k) to facilitate the alignment of European cybersecurity certification schemes with internationally recognised standards, including as part of the maintenance of existing European cybersecurity certification schemes and, where appropriate, to make recommendations to ENISA to engage with relevant European or international standardisation organisations to address insufficiencies or gaps in available European or internationally recognised standards.
Article 90(3), point (ka)		
1018a		*(ka) to assist, advise and cooperate with the Commission and ENISA in relation to the international recognition of cybersecurity certificates pursuant to Article 87.*
Article 90(4)		
1019	4. With the assistance of ENISA, the Commission shall chair the ECCG and provide the ECCG with a secretariat.	4. With the assistance of ENISA, the Commission shall chair the ECCG and provide the ECCG with a secretariat*, in accordance with the rules of procedure*

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
		adopted pursuant to Article 90(8).
Article 90(5)		
1020	5. The Commission may set up ECCG sub-groups for any of the following purposes:	5. *The ECCG, including upon request of* the Commission, may set up ECCG sub-groups for any of the following purposes:
Article 90(5), point (a)		
1021	(a) to examine specific questions on the basis of terms of reference established by the Commission;	(a) to examine specific questions on the basis of terms of reference established by the Commission;
Article 90(5), point (b)		
1022	(b) to maintain and review the European certification schemes in accordance with this Regulation and on the basis of terms of reference established by the Commission.	(b) to maintain and review the European certification schemes in accordance with this Regulation and on the basis of terms of reference established by the Commission.
Article 90(6)		
1023	6. The sub-groups shall report to the ECCG.	6. The sub-groups shall report to the ECCG *and shall cease to exist once they have fulfilled their mandate*.
Article 90(7)		
1024	7. The sub-groups shall be co-chaired by the Commission and ENISA, and the secretariat of the sub-groups shall be provided by ENISA.	7. The sub-groups shall be co-chaired by the Commission and ENISA, and the secretariat of the sub-groups shall be provided by ENISA.
Article 90(8)		
1025	8. The ECCG and its sub-groups shall adopt rules of procedure by simple majority of their members, based on a proposal by, and in agreement with the Commission.	8. The ECCG and its sub-groups shall adopt rules of procedure by simple majority of their members, based on a proposal by, and in agreement with the Commission.
Section 2		
1026	Section 2 Conformity assessment bodies	Section 2 Conformity assessment bodies
Article 91		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
1027	Article 91 Competence of conformity assessment bodies	Article 91 Competence of conformity assessment bodies
Article 91(1)		
1028	1. The conformity assessment bodies shall be accredited by national accreditation bodies appointed pursuant to Regulation (EC) No 765/2008. Such accreditation shall be issued only where the conformity assessment body meets the requirements set out in Annex I to this Regulation.	1. The conformity assessment bodies shall be accredited by national accreditation bodies appointed pursuant to Regulation (EC) No 765/2008. Such accreditation shall be issued only where the conformity assessment body meets the requirements set out in Annex I to this Regulation.
Article 91(2)		
1029	2. Where a European cybersecurity certificate is issued by a national cybersecurity certification authority pursuant to this Regulation, the certification body of the national cybersecurity certification authority shall be accredited as a conformity assessment body pursuant to paragraph 1.	2. Where a European cybersecurity certificate is issued by a national cybersecurity certification authority pursuant to this Regulation, the certification body of the national cybersecurity certification authority shall be accredited as a conformity assessment body pursuant to paragraph 1.
Article 91(3)		
1030	3. The accreditation referred to in paragraph 1 shall be issued to the conformity assessment bodies for a maximum of five years and may be renewed, provided that the conformity assessment body meets the requirements set out in this Article. National accreditation bodies shall take all appropriate measures within a reasonable timeframe to restrict, suspend or revoke the accreditation of a conformity assessment body issued pursuant to paragraph 1 where the conditions for the accreditation have not been met or are no longer met, or where the conformity assessment body does not comply with this Regulation.	3. The accreditation referred to in paragraph 1 shall be issued to the conformity assessment bodies for a maximum of five years and may be renewed, provided that the conformity assessment body meets the requirements set out in this Article. National accreditation bodies shall take all appropriate measures within a reasonable timeframe to restrict, suspend or revoke the accreditation of a conformity assessment body issued pursuant to paragraph 1 where the conditions for the accreditation have not been met or are no longer met, or where the conformity assessment body does not comply with this Regulation.
Article 91(4)		
1031	4. When establishing additional or specific accreditation requirements for a European cybersecurity certification scheme covering ICT products, pursuant to Article 92, synergies shall be sought, where appropriate, with the requirements relating to notified bodies under Regulation (EU) 2024/2847 and the accreditation requirements under the cybersecurity certification schemes which	4. When establishing additional or specific accreditation requirements for a European cybersecurity certification scheme covering ICT products, pursuant to Article 92, synergies shall be sought, where appropriate, with the requirements relating to notified bodies under Regulation (EU) 2024/2847 and the accreditation requirements under the cybersecurity certification schemes which

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	have already been adopted.	have already been adopted.
Article 91(5)		
1032	5. Where a conformity assessment body is accredited in accordance with Regulation (EU) 2024/2847, relevant authorities may reuse results from previous accreditation process regarding any overlapping requirements as evidence during the accreditation process under this Regulation.	5. Where a conformity assessment body is accredited in accordance with Regulation (EU) 2024/2847 *or other relevant Union legislation*, relevant authorities may reuse results from previous accreditation process regarding any overlapping requirements as evidence during the accreditation process under this Regulation.
Article 92		
1033	Article 92 Additional harmonisation of the competence of conformity assessment bodies	Article 92 Additional harmonisation of the competence of conformity assessment bodies
Article 92(1)		
1034	1. Where a European cybersecurity certification scheme sets out additional or specific requirements pursuant to Article 81(3), point (f), conformity assessment bodies shall be authorised by a national cybersecurity certification authority appointed pursuant to Article 88(1) to carry out tasks under such scheme. Such authorisation shall be issued only where the conformity assessment body has been accredited and meets the additional or specific requirements set out under the European cybersecurity certification scheme.	1. Where a European cybersecurity certification scheme sets out additional or specific requirements pursuant to Article 81(3), point (f), conformity assessment bodies shall be authorised by a national cybersecurity certification authority appointed pursuant to Article 88(1) to carry out tasks under such scheme. Such authorisation shall be issued only where the conformity assessment body has been accredited and meets the additional or specific requirements set out under the European cybersecurity certification scheme.
Article 92(2)		
1035	2. Where a conformity assessment body requests an authorisation under this Article, it shall submit the request to the national cybersecurity certification authority of the Member State in which it is established or with the national cybersecurity certification authority to which that Member State has had recourse in accordance with Article 88(1).	2. Where a conformity assessment body requests an authorisation under this Article, it shall submit the request to the national cybersecurity certification authority of the Member State in which it is established or with the national cybersecurity certification authority to which that Member State has had recourse in accordance with Article 88(1).
Article 92(3)		
1036	3. A conformity assessment body may request authorisation by a national cybersecurity certification authority other than that referred to in paragraph 2 in	3. A conformity assessment body may request authorisation by a national cybersecurity certification authority other than that referred to in paragraph 2 *if*

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	any one of the following situations:	*the national cybersecurity certification authority referred to in paragraph 1 does not perform authorisation in respect~~in any one~~* of the *~~following situations~~conformity assessment activities for which authorisation is sought*:
Article 92(3), point (a)		
1037	(a) where the national cybersecurity certification authority referred to in paragraph 1 does not perform authorisation in respect of the conformity assessment activities for which authorisation is sought;	(a) *~~where the national cybersecurity certification authority referred to in paragraph 1 does not perform authorisation in respect of the conformity assessment activities for which authorisation is sought;~~*
Article 92(3), point (b)		
1038	(b) where the national cybersecurity certification authority referred to in paragraph 1 has not undergone peer review in accordance with Article 89 in respect of the conformity assessment activities for which authorisation is sought.	(b) *~~where the national cybersecurity certification authority referred to in paragraph 1 has not undergone peer review in accordance with Article 89 in respect of the conformity assessment activities for which authorisation is sought.~~*
Article 92(4)		
1039	4. Where a national cybersecurity certification authority receives a request pursuant to paragraph 3, it shall inform the national cybersecurity certification authority of the Member State in which the requesting conformity assessment body is established. In such cases, the national cybersecurity certification authority of that Member State may participate in the authorisation as an observer.	4. Where a national cybersecurity certification authority receives a request pursuant to paragraph 3, it shall inform the national cybersecurity certification authority of the Member State in which the requesting conformity assessment body is established. In such cases, the national cybersecurity certification authority of that Member State may participate in the authorisation as an observer.
Article 92(5)		
1040	5. A national cybersecurity certification authority may request another national cybersecurity certification authority to carry out parts of the assessment activity. In such a case, the authorisation certificate shall be issued by the requesting authority.	5. A national cybersecurity certification authority may request another national cybersecurity certification authority to carry out parts of the assessment activity. In such a case, the authorisation certificate shall be issued by the requesting authority.
Article 92(6)		
1041	6. The authorisation referred to in paragraph 1 shall be valid for a period no longer than the period of validity of the accreditation, and may be renewed provided that the conformity assessment body meets the requirements set out in	6. The authorisation referred to in paragraph 1 shall be valid for a period no longer than the period of validity of the accreditation, and may be renewed provided that the conformity assessment body meets the requirements set out in

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	paragraph 1 and its accreditation has also been renewed.	paragraph 1 and its accreditation has also been renewed.
Article 92(7)		
1042	7. National cybersecurity certification authorities shall, within a reasonable timeframe, take all appropriate measures to restrict, suspend or revoke the authorisation of a conformity assessment body issued pursuant to paragraph 1 where the conditions for the authorisation have not been met or are no longer met, or where the conformity assessment body does not comply with this Regulation.	7. National cybersecurity certification authorities shall, within a reasonable timeframe, take all appropriate measures to restrict, suspend or revoke the authorisation of a conformity assessment body issued pursuant to paragraph 1 where the conditions for the authorisation have not been met or are no longer met, or where the conformity assessment body does not comply with this Regulation.
Article 92(8)		
1043	8. The Commission is empowered to adopt implementing acts to lay down the procedures, including on cross-border cooperation, for authorisation of conformity assessment bodies. In the preparation process of implementing acts, the Commission shall consult ENISA and the ECCG. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2).	8. The Commission is empowered to adopt implementing acts to lay down the procedures, including on cross-border cooperation ***between national cybersecurity certification authorities***, for authorisation of conformity assessment bodies. In the preparation process of implementing acts, the Commission shall consult ENISA and the ECCG. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2).
Article 93		
1044	Article 93 Notification of conformity assessment bodies	Article 93 Notification of conformity assessment bodies
Article 93(1)		
1045	1. For each European cybersecurity certification scheme, the national cybersecurity certification authorities of a Member State shall notify the Commission and the other Member States of the conformity assessment bodies that have been accredited and, where applicable, authorised pursuant to Article 92.	1. For each European cybersecurity certification scheme, the national cybersecurity certification authorities of a Member State shall notify the Commission and the other Member States of the conformity assessment bodies that have been accredited and, where applicable, authorised pursuant to Article 92.
Article 93(2)		
1046	2. The national cybersecurity certification authorities shall carry out the notification as referred to in paragraph 1 using the electronic notification tool	2. The national cybersecurity certification authorities shall carry out the notification as referred to in paragraph 1 using the electronic notification tool

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	developed and managed by the Commission.	developed and managed by the Commission.
Article 93(3)		
1047	3. The Commission is empowered to adopt implementing acts to lay down the circumstances, formats and procedures for notifications referred to in paragraph 1 of this Article, including the objection procedure by other Member States during the notification process, the unique identification of conformity assessment bodies, as well as the circumstances for restriction, suspension or withdrawal of notification. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2).	3. The Commission is empowered to adopt implementing acts to lay down the circumstances, formats and procedures for notifications referred to in paragraph 1 of this Article, including the objection procedure by other Member States during the notification process, the unique identification of conformity assessment bodies, as well as the circumstances for restriction, suspension or withdrawal of notification. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2).
Article 94		
1048	Article 94 Challenges with regard to the competence of conformity assessment bodies	Article 94 Challenges with regard to the competence of conformity assessment bodies
Article 94(1)		
1049	1. The Commission shall investigate any cases in which it has doubts, or is made aware of doubts about the competence of a conformity assessment body to meet, or the continued fulfilment by a conformity assessment body of, the requirements and responsibilities to which it is subject.	1. The Commission shall investigate any cases in which it has doubts, or is made aware of doubts about the competence of a conformity assessment body to meet, or the continued fulfilment by a conformity assessment body of, the requirements and responsibilities to which it is subject.
Article 94(2)		
1050	2. The national cybersecurity certification authority shall provide the Commission, on request, with all information relating to the basis for the notification or the maintenance of the competence of the conformity assessment body concerned.	2. The national cybersecurity certification authority shall provide the Commission, on request, with all information relating to the basis for the notification or the maintenance of the competence of the conformity assessment body concerned.
Article 94(3)		
1051	3. The Commission shall ensure that all sensitive information obtained in the course of its investigations is treated confidentially.	3. The Commission shall ensure that all sensitive information obtained in the course of its investigations is treated confidentially.
Article 94(4)		

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
1052	4. Where the Commission ascertains that a conformity assessment body does not meet or no longer meets the requirements for its notification, it shall inform the national cybersecurity certification authority accordingly and request it to take the necessary corrective measures, including de-notification if necessary.	4. Where the Commission ascertains that a conformity assessment body does not meet or no longer meets the requirements for its notification, it shall inform the national cybersecurity certification authority accordingly and request it to take the necessary corrective measures, including de-notification if necessary.
Article 94(5)		
1053	5. Member States shall ensure that an appeal procedure against decisions of the notified bodies is available.	5. ~~*Member States shall ensure that an appeal procedure against decisions of the notified bodies is available.*~~
Article 94a		
1053a		*Article 94a* *Appeal against decisions of notified conformity assessment bodies* *Member States shall ensure that an appeal procedure against decisions of the notified conformity assessment bodies is available.* See also Recital 127(a).
Article 95		
1054	Article 95 Information and retention obligation on conformity assessment bodies	Article 95 Information and retention obligation on conformity assessment bodies
Article 95(1)		
1055	1. Conformity assessment bodies shall inform the national cybersecurity certification authority of the following:	1. Conformity assessment bodies shall inform the national cybersecurity certification authority of the following:
Article 95(1), point (a)		
1056	(a) any refusal, restriction, suspension or withdrawal of a certificate;	(a) any *issuance,* refusal, restriction, suspension or withdrawal of a certificate;
Article 95(1), point (b)		
1057	(b) any circumstances affecting the scope of and conditions for the notification	(b) any circumstances affecting the scope of and conditions for the notification

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	referred to in Article 93(1);	referred to in Article 93(1);
Article 95(1), point (c)		
1058	(c) any request for information that they have received from market surveillance authorities regarding conformity assessment activities;	(c) any request for information that they have received from market surveillance authorities regarding conformity assessment activities;
Article 95(1), point (d)		
1059	(d) on request, any conformity assessment activities performed within the scope of their notification and any other activity performed, including cross-border activities and subcontracting.	(d) on request, any conformity assessment activities performed within the scope of their notification and any other activity performed, including cross-border activities and subcontracting.
Article 95(2)		
1060	2.Conformity assessment bodies shall also provide ENISA with the information referred to in paragraph 1 point (a) in view of facilitating the performance of its task under Article 79.	2.Conformity assessment bodies shall also ~~*provide*~~***inform*** ENISA ~~*with the information referred to in paragraph 1 point (a) in view of facilitating the performance of its task under Article 79*~~***on any issuance, restriction, suspension or withdrawal of a certificate**.
Article 95(3)		
1061	3.Conformity assessment bodies shall provide the other conformity assessment bodies under this Regulation carrying out similar conformity assessment activities covering the same ICT products, ICT services, ICT processes, managed security services or entities the cyber posture of which is certified without undue delay with relevant information on issues relating to negative and, upon request, positive conformity assessment results.	3.Conformity assessment bodies shall provide the other conformity assessment bodies under this Regulation carrying out similar conformity assessment activities covering the same ICT products, ICT services, ICT processes, managed security services or entities the cyber posture of which is certified without undue delay with relevant information on issues relating to negative and, upon request, positive conformity assessment results.
Article 95(4)		
1062	4.Conformity assessment bodies shall maintain a record system, containing all the documents and evidence produced or received in connection with each evaluation and certification that they perform. The record shall be stored in a secure and accessible manner for the period necessary for the purposes of certification and for at least five years after the expiry or withdrawal of a relevant European cybersecurity certificate.	4.Conformity assessment bodies shall maintain a record system, containing all the documents and evidence produced or received in connection with each evaluation and certification that they perform. The record shall be stored in a secure and accessible manner for the period necessary for the purposes of certification and for at least five years after the expiry or withdrawal of a relevant European cybersecurity certificate.

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
Section 3		
1063	Section 3 Other provisions	Section 3 Other provisions
Article 96		
1064	Article 96 Rights to lodge a complaint and right to an effective judicial remedy	Article 96 Rights to lodge a complaint and right to an effective judicial remedy
Article 96(1)		
1065	1. Natural and legal persons shall have the right to lodge a complaint with the issuer of a European cybersecurity certificate or, where the complaint relates to a European cybersecurity certificate issued by a conformity assessment body when acting in accordance with Article 85(4), with the relevant national cybersecurity certification authority.	1. Natural and legal persons shall have the right to lodge a complaint with the issuer of a European cybersecurity certificate or, where the complaint relates to a European cybersecurity certificate issued by a conformity assessment body when acting in accordance with Article ~~85(4)~~ ***85(3), point (ba)***, with the relevant national cybersecurity certification authority.
Article 96(2)		
1066	2. The authority or body with which the complaint has been lodged shall inform the complainant of the progress of the proceedings, of the decision taken, and of the right to an effective judicial remedy referred to in paragraphs 3 and 4.	2. The authority or body with which the complaint has been lodged shall inform the complainant of the progress of the proceedings, of the decision taken, and of the right to an effective judicial remedy referred to in paragraphs 3 and 4.
Article 96(3)		
1067	3. Notwithstanding any administrative or other non-judicial remedies, natural and legal persons shall have the right to an effective judicial remedy with regard to:	3. Notwithstanding any administrative or other non-judicial remedies, natural and legal persons shall have the right to an effective judicial remedy with regard to:
Article 96(3), point (a)		
1068	(a) decisions taken by the authority or body referred to in paragraph 1 including, where applicable, in relation to the improper issuing, failure to issue or recognition of a European cybersecurity certificate held by those natural and legal persons;	(a) decisions taken by the authority or body referred to in paragraph 1 including, where applicable, in relation to the improper issuing, failure to issue or recognition of a European cybersecurity certificate held by those natural and legal persons;
Article 96(3), point (b)		
1069	(b) a failure to act on a complaint lodged with the authority or body referred to in	(b) a failure to act on a complaint lodged with the authority or body referred to in

PUBLIC

	CLEAN Commission Proposal	VS.EC Council Mandate
	paragraph 1.	paragraph 1.
Article 96(4)		
1070	4. Proceedings pursuant to this Article shall be brought before the courts of the Member State in which the authority or body against which the judicial remedy is sought is located.	4. Proceedings pursuant to this Article shall be brought before the courts of the Member State in which the authority or body against which the judicial remedy is sought is located.
Article 97		
1071	Article 97 Penalties	Article 97 Penalties
Article 97, first paragraph		
1072	Member States shall lay down the rules on penalties applicable to infringements of this Title and to infringements of European cybersecurity certification schemes, and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall without delay notify the Commission of those rules and of those measures and shall notify it of any subsequent amendment affecting them.	Member States shall lay down the rules on penalties applicable to infringements of this Title and to infringements of European cybersecurity certification schemes, and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall without delay notify the Commission of those rules and of those measures and shall notify it of any subsequent amendment affecting them.

PUBLIC