



Council of the
European Union

Brussels, 18 April 2023
(OR. en)

8332/23

**Interinstitutional File:
2022/0085(COD)**

LIMITE

**CYBER 87
TELECOM 104
INST 122
CSC 175
CSCI 52
INF 71
FIN 427
BUDGET 4
DATAPROTECT 104
CODEC 614**

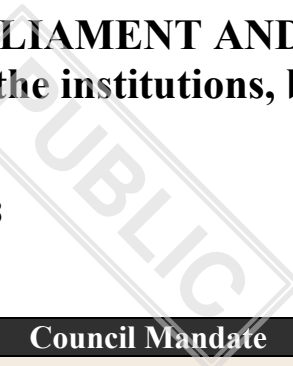
NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	14128/22 + ADD 1; 7656/23
No. Cion doc.:	7474/22 + ADD 1
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union - 4-column table

Delegations will find in the Annex a four-column table concerning the above legislative proposal, as it results from technical meetings held on 21, 23 and 28 March, 13 and 14 April.

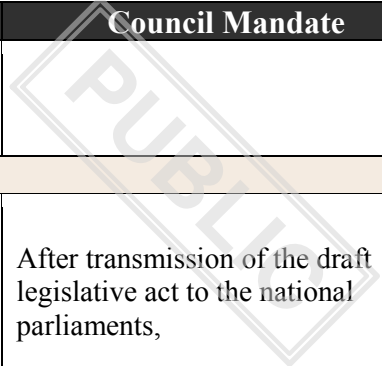
Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union

2022/0085(COD)
18-04-2023 at 13h28



	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Formula				
1	2022/0085 (COD)	2022/0085 (COD)	2022/0085 (COD)	2022/0085 (COD) Text Origin: Commission Proposal
Proposal Title				
2	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union Text Origin: Commission Proposal
Formula				
3				

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, Text Origin: Commission Proposal
Citation 1				
4	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 298 thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 298 thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 298 thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 298 thereof, Text Origin: Commission Proposal
Citation 2				
5	Having regard to the Treaty establishing the European Atomic Energy Community, and in particular Article 106a thereof,	Having regard to the Treaty establishing the European Atomic Energy Community, and in particular Article 106a thereof,	Having regard to the Treaty establishing the European Atomic Energy Community, and in particular Article 106a thereof,	Having regard to the Treaty establishing the European Atomic Energy Community, and in particular Article 106a thereof, Text Origin: Commission Proposal
Citation 3				
6	Having regard to the proposal from the European Commission,	Having regard to the proposal from the European Commission,	Having regard to the proposal from the European Commission,	Having regard to the proposal from the European Commission,




	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
				Text Origin: Commission Proposal
Citation 4				
7	After transmission of the draft legislative act to the national parliaments,	After transmission of the draft legislative act to the national parliaments,	After transmission of the draft legislative act to the national parliaments,	After transmission of the draft legislative act to the national parliaments, Text Origin: Commission Proposal
Citation 5				
8	Acting in accordance with the ordinary legislative procedure,	Acting in accordance with the ordinary legislative procedure,	Acting in accordance with the ordinary legislative procedure,	Acting in accordance with the ordinary legislative procedure, Text Origin: Commission Proposal
Formula				
9	Whereas:	Whereas:	Whereas:	Whereas: Text Origin: Commission Proposal
Recital 1				
10	(1) In the digital age, information and communication technology is a	(1) In the digital age, information and communication technology is a	(1) In the digital age, information and communication technology is a	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	cornerstone in an open, efficient and independent Union administration. Evolving technology and increased complexity and interconnectedness of digital systems amplify cybersecurity risks making the Union administration more vulnerable to cyber threats and incidents, which ultimately poses threats to the administration's business continuity and capacity to secure its data. While increased use of cloud services, ubiquitous use of IT, high digitalisation, remote work and evolving technology and connectivity are nowadays core features of all activities of the Union administration entities, digital resilience is not yet sufficiently built in.	cornerstone in an open, efficient and independent Union administration. Evolving technology and increased complexity and interconnectedness of digital systems amplify cybersecurity risks making the Union administration more vulnerable to cyber threats and incidents, which ultimately poses threats to the administration's business continuity and capacity to secure its data. While increased use of cloud services, the ubiquitous use of IT information and communication technology (ICT) , high digitalisation, remote work and evolving technology and connectivity are nowadays core features of all activities of the Union administration entities, digital resilience is not yet sufficiently built in.	cornerstone in an open, efficient and independent Union administration. Evolving technology and increased complexity and interconnectedness of digital systems amplify cybersecurity risks making the Union administration more vulnerable to cyber threats and incidents, which ultimately poses threats to the administration's business continuity and capacity to secure its data. While increased use of cloud services, ubiquitous use of IT, high digitalisation, remote work and evolving technology and connectivity are nowadays core features of all activities of the Union administration entities, digital resilience is not yet sufficiently built in.	
Recital 2				
11	(2) The cyber threat landscape faced by Union institutions, bodies and agencies is in constant evolution. The tactics, techniques and procedures employed by threat actors are constantly evolving, while the prominent motives for	(2) The cyber threat landscape faced by Union institutions, bodies and agencies entities is in constant evolution. The tactics, techniques and procedures employed by threat actors are constantly evolving, while the prominent motives for	(2) The cyber threat landscape faced by Union institutions, bodies and agencies entities is in constant evolution. The tactics, techniques and procedures employed by threat actors are constantly evolving, while the prominent motives for	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	such attacks change little, from stealing valuable undisclosed information to making money, manipulating public opinion or undermining digital infrastructure. The pace at which they conduct their cyberattacks keeps increasing, while their campaigns are increasingly sophisticated and automated, targeting exposed attack surfaces that keep expanding and quickly exploiting vulnerabilities.	such attacks change little, from stealing valuable undisclosed information to making money, manipulating public opinion or undermining digital infrastructure. The pace at which they conduct their cyberattacks keeps increasing, while their campaigns are increasingly sophisticated and automated, targeting exposed attack surfaces that keep expanding and quickly exploiting vulnerabilities.	such attacks change little, from stealing valuable undisclosed information to making money, manipulating public opinion or undermining digital infrastructure. The pace at which they conduct their cyberattacks keeps increasing, while their campaigns are increasingly sophisticated and automated, targeting exposed attack surfaces that keep expanding and quickly exploiting vulnerabilities.	
Recital 3				
12	(3) The Union institutions, bodies and agencies' IT environments have interdependencies, integrated data flows and their users collaborate closely. This interconnection means that any disruption, even when initially confined to one Union institution, body or agency, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts on the others. In addition, certain institutions, bodies and agencies' IT environments are connected with Member States' IT environments, causing an incident	(3) The Union institutions, bodies and agencies' IT entities' ICT environments have interdependencies, integrated data flows and their users collaborate closely. This interconnection means that any disruption, even when initially confined to one Union institution, body or agency entity , can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts on the others. In addition, certain institutions, bodies and agencies' Union entities' ICT environments are connected with	(3) The Union institutions, bodies and agencies' entities' IT environments have interdependencies, integrated data flows and their users collaborate closely. This interconnection means that any disruption, even when initially confined to one Union institution, body or agency entity , can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts on the others. In addition, certain institutions, bodies and agencies' Union entities' IT environments are connected with Member States' IT	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	in one Union entity to pose a risk to the cybersecurity of Member States' IT environments and vice versa.	Member States' IT environments, causing an incident in one Union entity to pose a risk to the cybersecurity of Member States' IT environments and vice versa.	environments, causing an incident in one Union entity to pose a risk to the cybersecurity of Member States' IT environments and vice versa. Furthermore, Union entities handle large amounts of often sensitive information from Member States, therefore incidents could negatively affect Member States as well. For this reason, the cybersecurity of the Union entities is of high importance for the Member States as well. Incident-specific information may also facilitate the detection of similar cyber threats or incidents affecting Member States.	
Recital 4				
13	(4) The Union institutions, bodies and agencies are attractive targets who face highly skilled and well-resourced threat actors as well as other threats. At the same time, the level and maturity of cyber resilience and the ability to detect and respond to malicious cyber activities varies significantly across those entities. It is thus necessary for the functioning of the European administration that the institutions,	(4) The Union institutions, bodies and agencies entities are attractive targets who face highly skilled and well-resourced threat actors as well as other threats. At the same time, the level and maturity of cyber resilience and the ability to detect and respond to malicious cyber activities varies significantly across those entities. It is thus necessary for the functioning of the European administration that the institutions,	(4) The Union institutions, bodies and agencies entities are attractive targets who face highly skilled and well-resourced threat actors as well as other threats. At the same time, the level and maturity of cyber resilience and the ability to detect and respond to malicious cyber activities varies significantly across those entities. It is thus necessary for the functioning of the European administration that the institutions,	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	bodies and agencies of the Union achieve a high common level of cybersecurity through a cybersecurity baseline (a set of minimum cybersecurity rules with which network and information systems and their operators and users have to be compliant to minimise cybersecurity risks), information exchange and collaboration.	bodies and agencies of the Union Union entities achieve a high common level of cybersecurity through a cybersecurity baseline (a set of minimum cybersecurity rules with which network and information systems and their operators and users have to be compliant to minimise cybersecurity risks) the implementation of cybersecurity rules with which network and information systems and their operators and users have to be compliant to minimise cybersecurity risk-management measures commensurate with the relevant risks), information exchange and collaboration.	bodies and agencies of the Union entities achieve a high common level of cybersecurity through a cybersecurity baseline (a set of minimum cybersecurity rules with which network and information systems and their operators and users have to be compliant to minimise cybersecurity risks) implementation of cybersecurity rules with which network and information systems and their operators and users have to be compliant to minimise cybersecurity risks), information exchange and collaboration.	
Recital 5				
14	(5) The Directive [proposal NIS 2] on measures for a high common level of cybersecurity across the Union aims to further improve the cybersecurity resilience and incident response capacities of public and private entities, national competent authorities and bodies as well as the Union as a whole. It is therefore necessary that Union institutions, bodies and agencies follow suit by ensuring rules that are consistent with the Directive [proposal NIS 2] and mirror its level of ambition.	(5) The Directive [proposal NIS 2] on measures for a high common level of cybersecurity across the Union (EU) 2022/2555 of the European Parliament and of the Council ¹ aims to further improve the cybersecurity resilience and incident response capacities of public and private entities, national competent authorities and bodies as well as the Union as a whole. It is therefore necessary that Union institutions, bodies and agencies entities follow suit by ensuring rules that are consistent with the Directive [proposal NIS 2]	(5) The Directive [proposal NIS 2] on measures for a high common level of cybersecurity across the Union aims to further improve the cybersecurity resilience and incident response capacities of public and private entities, national competent authorities and bodies as well as the Union as a whole. It is therefore necessary that Union institutions, bodies and agencies entities follow suit by ensuring rules that are consistent with the Directive [proposal NIS 2] and mirror its level of ambition.	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		<p>(EU) 2022/2555 and mirror its level of ambition.</p> <p>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).</p>		
Recital 6				
15	<p>(6) To reach a high common level of cybersecurity, it is necessary that each Union institution, body and agency establishes an internal cybersecurity risk management, governance and control framework that ensures an effective and prudent management of all cybersecurity risks, and takes account of business continuity and crisis management.</p>	<p>(6) To reach a high common level of cybersecurity, it is necessary that each Union institution, body and agency entity establishes an internal cybersecurity risk management, handling of incidents, governance and control framework that ensures an effective and prudent management of all cybersecurity risks, and takes account of business continuity and crisis management. That framework should lay down cybersecurity policies and priorities for the security of network and information systems encompassing the entirety of the ICT environment. The framework should be reviewed on a regular basis and</p>	<p>(6) To reach a high common level of cybersecurity, it is necessary that each Union institution, body and agency entity establishes an internal cybersecurity risk management, governance and control framework that ensures an effective and prudent management of all cybersecurity risks . The framework should lay down cybersecurity policies, including procedures to assess the effectiveness of implemented cybersecurity measures. The framework should be based on an all-hazard approach, which aims to protect network and information systems and the physical environment of those systems from events such as</p>	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
		at least every three years.	theft, fire, flood, telecommunication or power failures, or unauthorised physical access and damage to, and interference with Union entity's information and information processing facilities, which could compromise the availability, authenticity, integrity or confidentiality of data stored, transmitted, processed or accessible via network and information systems. The framework should reflect the findings of the risk analysis, taking and takes account of business continuity and crisis management all the relevant technical, operational and organisational risks to the cybersecurity of the concerned Union entity.	
15a			(6a) To manage the risks identified under the framework, each Union entity should ensure that appropriate and proportionate technical, operational and organisational measures are taken. These should address the domains,	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			including cybersecurity measures set out in this Regulation to strengthen the cybersecurity of each Union entity.	
15b			(6b) The assets and risks identified in the framework as well as conclusions derived from regular maturity assessments should be reflected in cybersecurity plan established by each Union entity. The cybersecurity plan should include the adopted cybersecurity measures, with the aim to increase the overall cybersecurity of the concerned Union entity.	
15c			(6c) As ensuring cybersecurity is a continuous process, the suitability and effectiveness of all measures should be regularly revised in light of the changing risks, assets and maturity of the Union entities. The framework should be reviewed on a regular basis and at least every three years, while the cybersecurity	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			plan should be revised at least every two years or following each maturity assessment or every review of the framework.	
15d			(6d) Union entities should exchange relevant information on a regular basis, including with regard to relevant incidents and cyber threats, while ensuring the confidentiality and appropriate protection of the information provided by the reporting Union entity.	
15e			(6e) A mechanism to ensure effective exchange of information, coordination, and cooperation of the Union entities in case of major incidents should be implemented, including a clear identification of the roles and responsibilities of the involved Union entities. The information exchanged should be taken into account by the designated point of contact for EU-CyCLONe, when sharing	

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
			relevant information with EU-CyCLONe as a contribution to the shared situational awareness.	

Recital 7				
16	<p>(7) The differences between Union institutions, bodies and agencies require flexibility in the implementation since one size will not fit all. The measures for a high common level of cybersecurity should not include any obligations directly interfering with the exercise of the missions of Union institutions, bodies and agencies or encroaching on their institutional autonomy. Thus, those institutions, bodies and agencies should establish their own frameworks for cybersecurity risk management, governance and control, and adopt their own baselines and cybersecurity plans.</p>	<p>(7) The differences between Union institutions, bodies and agenciesentities require flexibility in the implementation since one size will not fit all. The measures for a high common level of cybersecurity should not include any obligations directly interfering with the exercise of the missions of Union institutions, bodies and agenciesentities or encroaching on their institutional autonomy. ThusTherefore, those institutions, bodies and agenciesentities should establish their own frameworks for cybersecurity risk management, handling of incidents, governance and control, and adopt their own baselinescybersecurity risk-management measures and cybersecurity plans, covering the entity's entire ICT environment. Union entities should continuously evaluate the effectiveness of the adopted risk-management measures and their proportionality relative to the identified risks, and where necessary, adjust and revise accordingly their frameworks</p>	<p>(7) The differences between Union institutions, bodies and agenciesentities require flexibility in the implementation since one size will not fit all. The measures for a high common level of cybersecurity should not include any obligations directly interfering with the exercise of the missions of Union institutions, bodies and agenciesentities or encroaching on their institutional autonomy. Thus, those institutions, bodies and agenciesUnion entities should establish their own frameworks for cybersecurity risk management, governance and control and cybersecurity plans. When implementing such measures, due account should be taken of synergies existing between Union entities, with the aim of proper management of resources and cost optimisation. Due account should also be taken that the measures do not negatively affect the Union entities' efficient information exchange and operations with other Union</p>	


		and plans on the basis of the results of the cybersecurity maturity assessments.	entities and national competent authorities their own baselines and cybersecurity plans.	
16a		(7a) The recurrent obligation to carry out cybersecurity maturity assessments could create an additional and disproportionate burden for small Union entities with limited ICT resources. This Regulation should therefore provide for the possibility for two or more Union entities to create joint teams for carrying out the cybersecurity maturity assessments, and benefit from combining resources and expertise.		
Recital 8				
17	(8) In order to avoid imposing a disproportionate financial and administrative burden on Union institutions, bodies and agencies, the cybersecurity risk management requirements should be proportionate to the risk presented by the network and information system concerned, taking into account the state of the art of such	(8) In order to avoid imposing a disproportionate financial and administrative burden on Union institutions, bodies and agencies, entities , the cybersecurity risk management risk-management requirements should be proportionate to the risk presented by the network and information system concerned, taking into	(8) In order to avoid imposing a disproportionate financial and administrative burden on Union institutions, bodies and agencies entities , the cybersecurity risk management requirements should be proportionate to the risk presented by the network and information system concerned, taking into account the state of the	

	measures. Each Union institution, body and agency should aim to allocate an adequate percentage of its IT budget to improve its level of cybersecurity; in the longer term a target in the order of 10% should be pursued.	account the state of the art of such measures. Each Union institution, body and agency entity should aim to allocate an adequate percentage of its IT budget to improve its level of cybersecurity; in the longer term a target in the order of at least 10% should be pursued.	art of such measures. Each Union institution, body and agency entity should aim to allocate an adequate percentage of its IT budget to improve its level of cybersecurity; in the longer term a target in the order of 10% should be pursued. The maturity assessment should also assess whether the Union entity's cybersecurity spending is proportionate to the risks it faces.	
Recital 9				
18	(9) A high common level of cybersecurity requires cybersecurity to come under the oversight of the highest level of management of each Union institution, body and agency, who should approve a cybersecurity baseline that should address the risks identified under the framework to be established by each institution, body and agency. Addressing the cybersecurity culture, i.e. the daily practice of cybersecurity, is an integral part of a cybersecurity baseline in all Union institutions, bodies and agencies.	(9) A high common level of cybersecurity requires cybersecurity to come under the oversight of the highest level of management of each Union institution, body and agency, who should approve a entity, who should oversee the implementation of the provisions of this Regulation and approve the establishment, and any subsequent revisions thereof, of the risk management and control framework, the corresponding cybersecurity baseline that should address risk-management measures addressing the risks identified under in the framework to be established by each	(9) A high common level of cybersecurity requires cybersecurity to come under the oversight of the highest level of management of each Union entity. institution, body and agency, who should approve a cybersecurity baseline that should address the risks identified under the framework to be established by each institution, body and agency oversee the implementation of this Regulation, including establishment of the risk management, governance and control framework and cybersecurity plans,	

		<p>institution, body and agency and the cybersecurity plans of each Union entity. Addressing the cybersecurity culture, i.e. the daily practice of cybersecurity, is an integral part of a cybersecurity baseline in all Union institutions, bodies and agencies risk-management, governance and control framework and the corresponding cybersecurity risk-management measures in all Union entities.</p>	<p>encompassing cybersecurity measures. Addressing the cybersecurity culture, i.e. the daily practice of cybersecurity, is an integral part of a cybersecurity baseline framework in all Union institutions, bodies and agencies entities .</p>	
Recital 10				
19	<p>(10) Union institutions, bodies and agencies should assess risks related to relationships with suppliers and service providers, including providers of data storage and processing services or managed security services, and take appropriate measures to address them. These measures should form part of the cybersecurity baseline and be further specified in guidance documents or recommendations issued by CERT-EU. When defining measures and guidelines, due account should be taken of relevant EU legislation and policies, including risk assessments and recommendations</p>	<p>(10) Union institutions, bodies and agencies entities should assess risks related to relationships with suppliers and service providers, including providers of data storage and processing services or managed security services, and take appropriate measures to address them. These measures should form part of the cybersecurity baseline and risk-management measures should be further specified in guidance documents or recommendations issued by CERT-EU. When defining measures and guidelines, due account should be taken of relevant EU legislation Union law</p>	<p>(10) Union institutions, bodies and agencies Cybersecurity should assess risks related to relationships with suppliers and service providers, including providers of data storage and processing services or managed security services, and take appropriate measures to address them. These measures should form part of the cybersecurity baseline plan and be further specified in guidance documents or recommendations issued by CERT-EU. When defining measures and guidelines, due account should be taken of the state of the art and, where applicable, relevant European</p>	

	<p>issued by the NIS Cooperation Group, such as the EU Coordinated risk assessment and EU Toolbox on 5G cybersecurity. In addition, certification of relevant ICT products, services and processes could be required, under specific EU cybersecurity certification schemes adopted pursuant to Article 49 of Regulation EU 2019/881.</p>	<p>and policies, including risk assessments and recommendations issued by the NIS Cooperation Group established by Directive (EU) 2022/2555, such as the EU Coordinated risk assessment and EU Toolbox on 5G cybersecurity. In addition, considering the threat landscape and the importance of building up resilience for the Union entities certification of relevant ICT products, services and processes couldmust be required, under specific EUUnion cybersecurity certification schemes adopted pursuant to Article 49 of Regulation EU 2019/881.</p>	<p>and international standards, as well as relevant EU legislation and policies, including risk assessments and recommendations issued by the NIS Cooperation Group, such as the EU Coordinated risk assessment and EU Toolbox on 5G cybersecurity. In addition, certification of relevant ICT products, services and processes could be required, under specific EU cybersecurity certification schemes adopted pursuant to Article 49 of Regulation EU 2019/881. Where appropriate, CERT-EU should cooperate with ENISA.</p>	
Recital 11				
20	<p>(11) In May 2011, the Secretaries-General of the Union institutions and bodies decided to establish a pre-configuration team for a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU) supervised by an inter-institutional Steering Board. In July 2012, the Secretaries-General confirmed the practical arrangements and agreed to maintain CERT-EU as a permanent entity to continue to help improve the overall level of</p>	<p>(11) In May 2011, the Secretaries-General of the Union institutions and bodies decided to establish a pre-configuration team for a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU) supervised by an inter-institutional Steering Board. In July 2012, the Secretaries-General confirmed the practical arrangements and agreed to maintain CERT-EU as a permanent entity to continue to help improve the overall level of</p>	<p>(11) In May 2011, the Secretaries-General of the Union institutions and bodies decided to establish a pre-configuration team for a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU) supervised by an inter-institutional Steering Board. In July 2012, the Secretaries-General confirmed the practical arrangements and agreed to maintain CERT-EU as a permanent entity to continue to help improve the overall level of</p>	

	<p>information technology security of the Union’s institutions, bodies and agencies as an example of visible inter-institutional cooperation in cybersecurity. In September 2012, CERT-EU was established as a Taskforce of the European Commission with an interinstitutional mandate. In December 2017, the Union institutions and bodies concluded an interinstitutional arrangement on the organisation and operation of CERT-EU¹. This arrangement should continue to evolve to support the implementation of this Regulation.</p> <p>¹. OJ C 12, 13.1.2018, p. 1–11.</p>	<p>information technology security of the Union’s institutions, bodies and agencies as an example of visible inter-institutional cooperation in cybersecurity. In September 2012, CERT-EU was established as a Taskforce of the European Commission with an interinstitutional mandate. In December 2017, the Union institutions and bodies concluded an interinstitutional arrangement on the organisation and operation of CERT-EU¹. ThisThat arrangement should continue to evolve to support the implementation of this Regulation and should be evaluated on a regular basis in light of future negotiations of long-term budget frameworks allowing for further decisions to be made with respect to the functioning and institutional role of CERT-EU, including the possible establishment of CERT-EU as a Union office.</p> <p>¹. OJ C 12, 13.1.2018, p. 1–11.</p>	<p>information technology security of the Union’s institutions, bodies and agencies as an example of visible inter-institutional cooperation in cybersecurity. In September 2012, CERT-EU was established as a Taskforce of the European Commission with an interinstitutional mandate. In December 2017, the Union institutions and bodies concluded an interinstitutional arrangement on the organisation and operation of CERT-EU¹. This arrangementCERT- EU¹. This Regulation should provide a comprehensive set of rules on the organisation, functioning and operation of CERT-EU. The provisions continue to evolve to support the implementation of this Regulation prevail over provisions of the interinstitutional arrangement on the organisation and operation of CERT-EU that was concluded in December 2017.</p> <p>¹. OJ C 12, 13.1.2018, p. 1–11.</p>	
Recital 12				
21	(12) CERT-EU should be renamed from ‘computer emergency	(12) CERT-EU should be renamed from ‘computer emergency	<i>deleted</i>	

	response team’ to ‘Cybersecurity Centre’ for the Union institutions, bodies and agencies, in line with developments in the Member States and globally, where many CERTs are renamed as Cybersecurity Centres, but it should keep the short name ‘CERT-EU’ because of name recognition.	response team’ to ‘Cybersecurity Centre’ for the Union institutions, bodies and agencies entities , in line with developments in the Member States and globally, where many CERTs are renamed as Cybersecurity Centres, but it should keep the short name ‘CERT-EU’ because of name recognition.		
<i>Recital 13</i>				
22	(13) Many cyberattacks are part of wider campaigns that target groups of Union institutions, bodies and agencies or communities of interest that include Union institutions, bodies and agencies. To enable proactive detection, incident response or mitigating measures, Union institutions, bodies and agencies should notify CERT-EU of significant cyber threats, significant vulnerabilities and significant incidents and share appropriate technical details that enable detection or mitigation of, as well as response to, similar cyber threats, vulnerabilities and incidents in other Union institutions, bodies and agencies. Following the same approach as the one envisaged in Directive	(13) Many cyberattacks are part of wider campaigns that target groups of Union institutions, bodies and agencies entities or communities of interest that include Union institutions, bodies and agencies entities . To enable proactive detection, incident response or mitigating measures, Union institutions, bodies and agencies and recovery from significant incidents, Union entities should notify CERT-EU of significant cyber threats, significant vulnerabilities, near misses and significant incidents and share appropriate technical details that enable detection or mitigation of, as well as response to, similar cyber threats, vulnerabilities and and recovery	(13) Many cyberattacks are part of wider campaigns that target groups of Union institutions, bodies and agencies entities or communities of interest that include Union institutions, bodies and agencies entities . To enable proactive detection, incident response or mitigating measures, Union institutions, bodies and agencies entities should notify CERT-EU of significant cyber threats, significant vulnerabilities, near misses and and significant incidents and share appropriate technical details that enable detection or mitigation of, as well as response to, similar cyber threats, vulnerabilities, near misses and incidents in other Union institutions, bodies and	

	<p>[proposal NIS 2], where entities become aware of a significant incident they should be required to submit an initial notification to CERT-EU within 24 hours. Such information exchange should enable CERT-EU to disseminate the information to other Union institutions, bodies and agencies, as well as to appropriate counterparts, to help protect the Union IT environments and the Union’s counterparts’ IT environments against similar incidents, threats and vulnerabilities.</p>	<p>from similar incidents in other Union institutions, bodies and agenciesentities. Following the same approach as the one envisaged in Directive [proposal NIS 2](EU) 2022/2555, where entities become aware of a significant incident they should be required to submit an initial notificationearly warning to CERT-EU within 24 hours. Such information exchange should enable CERT-EU to disseminate the information to other Union institutions, bodies and agenciesentities, as well as to appropriate counterparts, to help protect the Union ITFICT environments and the Union’s counterparts’ ITFICT environments against similar incidents, threats and vulnerabilities.</p>	<p>agenciesentities. Following the same approach as the one envisaged in Directive [proposal NIS 2], where Union entities become aware of a significant incident they should be required to submit an initial notification early warning to CERT-EU within 24 hours. Such information exchange should enable CERT-EU to disseminate the information to other Union institutions, bodies and agenciesentities, as well as to appropriate counterparts, to help protect the Union IT environments and the Union’s counterparts’ IT environments against similar incidents, threats and vulnerabilities.</p>	
Recital 13				
22a		<p>(13a) This Regulation lays down a multiple-stage approach to the reporting of significant incidents in order to strike the right balance between, on the one hand, swift reporting that helps to mitigate the potential spread of incidents and that allows Union entities to seek assistance,</p>	<p>(13a) This Regulation lays down a multiple-stage approach to the reporting of significant incidents in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread of significant incidents and allows Union entities to seek assistance,</p>	

		<p>and, on the other, in-depth reporting that draws valuable lessons from individual incidents and improves over time the resilience of individual Union entities and contributes to increasing the overall cybersecurity posture of Union administration. In that regard, this Regulation should include the reporting of incidents that, based on an initial assessment performed by the Union entity concerned, could cause severe operational disruption of the services or financial loss for that Union entity or affect other natural or legal persons by causing considerable material or non-material damage. Such initial assessment should take into account, inter alia, the network and information systems affected, in particular their importance for the functioning and operations of the Union entity concerned, the severity and technical characteristics of a cyber threat and any underlying vulnerabilities that are being exploited as well as the experience of the Union entity concerned with similar incidents. Indicators such as the extent to</p>	<p>and, on the other hand, in-depth reporting that draws valuable lessons from individual incidents and improves over time the cyber resilience of individual Union entities. In that regard, this Regulation should include the reporting of incidents that, based on an initial assessment carried out by the Union entity, could cause severe operational disruption to the functioning of the Union entity or financial loss to the Union entity concerned or affect other natural or legal persons by causing considerable material or non-material damage. Such initial assessment should take into account, inter alia, the affected network and information systems, in particular their importance for the functioning of the Union entity, the severity and technical characteristics of a cyber threat and any underlying vulnerabilities that are being exploited as well as the Union entity's experience with similar incidents. Indicators such as the extent to which the functioning of the Union entity is affected, the duration of an incident or the number of affected natural or legal persons could play an</p>	
--	--	---	---	--

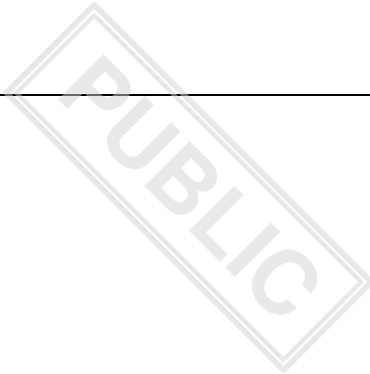
		<p>which the functioning of Union entity is affected, the duration of an incident or the number of users affected could play an important role in identifying whether the operational disruption of the service is severe.</p>	<p>important role in identifying whether the operational disruption is severe.</p>	
22b			<p>(13b) As the infrastructure and networks of the relevant Union entity and the Member State where that Union entity is located are interconnected, it is crucial for that Member State to be informed without undue delay of a significant incident within that Union entity. For that purpose, the affected Union entity should notify CERT-EU's national counterpart, designated by the Member State in accordance with the Directive [proposal NIS 2], in the same timeline as it should report a significant incident to CERT-EU. CERT-EU should also notify this national counterpart when it becomes aware of a significant incident within the Member State, unless already reported by the affected Union entity.</p>	

--	--	--	--	--


PUBLIC

Recital 14				
23	<p>(14) In addition to giving CERT-EU more tasks and an expanded role, an Interinstitutional Cybersecurity Board (IICB) should be established, which should facilitate a high common level of cybersecurity among Union institutions, bodies and agencies by monitoring the implementation of this Regulation by the Union institutions, bodies and agencies and by supervising implementation of general priorities and objectives by CERT-EU and providing strategic direction to CERT-EU. The IICB should ensure representation of the institutions and include representatives of agencies and bodies through the Union Agencies Network.</p>	<p>(14) In addition to giving CERT-EU more tasks and an expanded role, an Interinstitutional Cybersecurity Board (IICB) should be established, which should facilitate a high common level of cybersecurity among Union institutions, bodies and agenciesentities by monitoring the implementation of this Regulation by the Union institutions, bodies and agenciesentities and by supervising implementation of general priorities and objectives by CERT-EU and providing strategic direction to CERT-EU. The IICB should ensure representation of the institutions and include representatives of agencies and bodies through the Union Agencies Network.</p>	<p>(14) In addition to giving CERT-EU more tasks and an expanded role, an Interinstitutional Cybersecurity Board (IICB) should be established which, in order to, which should facilitate a high common level of cybersecurity among Union institutions, bodies and agenciesentities, should have an exclusive role in monitoring the implementation of this Regulation by the Union institutions, bodies and agenciesand by entities and in supervising implementation of general priorities and objectives by CERT-EU and providing strategic direction to CERT-EU. The IICB should therefore ensure representation of the institutions and include representatives of agencies and bodies through the Union Agencies Network. The organisation and functioning of the IICB should be further regulated by its internal rules of procedures that may include further specification of regular meetings of the IICB, including annual gatherings of the political</p>	

			<p>level where representatives of the highest level of management of each member of the IICB would allow for the IICB to have strategic discussion and provide strategic guidance of the IICB. Furthermore, the IICB may establish an Executive Committee to assist in its work and to delegate some of its tasks and powers to it, especially in terms of tasks that require specific expertise of its members, for instance the approval of the service catalogue and any subsequent updates to it, modalities for service level agreements, assessments of documents and reports submitted by the Union entities to the IICB according to this Regulation or tasks related to the preparation of decisions on compliance measures issued by the IICB and to monitoring of their implementation. The IICB should lay down the rules of procedures of the Executive Committee, including its tasks and powers.</p>	



23a		<p>(14a) The IICB aims to support entities in elevating their respective cybersecurity postures by implementing this Regulation. In order to support Union entities, the IICB should adopt guidance and recommendations required for Union entities' cybersecurity maturity assessments and cybersecurity plans, review possible interconnections between Union entities' ICT environments and support the establishment of a Cybersecurity Officers Group under ENISA, comprising the Local Cybersecurity Officers of all Union entities with an aim to facilitate the sharing of best practices and experiences gained from the implementation of this Regulation.</p>		
23b		<p>(14b) In order to ensure consistency with Directive (EU) 2022/2555, the IICB could adopt recommendations on the basis of the results of Union level</p>		

		<p>coordinated security risk assessments of critical supply chains referred to in Article 22 of Directive (EU) 2022/2555 to support Union entities in adopting effective and proportionate risk-management measures relating to supply chain security and develop guidelines for information sharing arrangements of Union entities relating to the voluntary notification of cyber threats, near misses and incidents to CERT-EU.</p>		
Recital 15				
24	<p>(15) CERT-EU should support the implementation of measures for a high common level of cybersecurity through proposals for guidance documents and recommendations to the IICB or by issuing calls for action. Such guidance documents and recommendations should be approved by the IICB. When needed, CERT-EU should issue calls for action describing urgent security measures which Union institutions, bodies and agencies are urged to take within a set timeframe.</p>	<p>(15) CERT-EU should support the implementation of measures for a high common level of cybersecurity through proposals for guidance documents and recommendations to the IICB or by issuing calls for action. Such guidance documents and recommendations should be approved by the IICB. When needed, CERT-EU should issue calls for action describing urgent security measures which Union institutions, bodies and agenciesentities are urged to take within a set timeframe.</p>	<p>(15) CERT-EU should support the implementation of measures for a high common level of cybersecurity through proposals for guidance documents and recommendations to the IICB or by issuing calls for action. Such guidance documents and recommendations should be approved by the IICB. When needed, CERT-EU should issue calls for action describing urgent security measures which Union institutions, bodies and agenciesentities are urged to take within a set timeframe. The IICB</p>	

			may instruct CERT-EU to issue, withdraw, or modify a proposal for guidance documents or recommendation, or a call for action.	
Recital 16				
25	(16) The IICB should monitor compliance with this Regulation as well as follow-up of guidance documents and recommendations, and calls for action issued by CERT-EU. The IICB should be supported on technical matters by technical advisory groups composed as the IICB sees fit which should work in close cooperation with CERT-EU, the Union institutions, bodies and agencies and other stakeholders as necessary. Where necessary, the IICB should issue non-binding warnings and recommend audits.	(16) The IICB should monitor compliance with this Regulation as well as follow-up of guidance documents and recommendations, and calls for action issued by CERT-EU. The IICB should be supported on technical matters by technical advisory groups, composed as the IICB sees fit which should work in close cooperation with CERT-EU, the Union institutions, bodies and agencies entities and other stakeholders as necessary appropriate . Where necessary, the IICB should issue non-binding warnings and recommend requests for audits.	(16) The IICB should monitor compliance with this Regulation as well as follow-up of guidance documents and recommendations, and calls for action issued by CERT-EU . The IICB should be supported on technical matters by technical advisory groups composed as the IICB sees fit which should work in close cooperation with CERT-EU, the Union institutions, bodies and agencies entities and other stakeholders as necessary. Where necessary, the IICB should issue non-binding warnings and recommend audits.	
25a		(16a) Where the IICB finds that a Union entity has not effectively applied or implemented this Regulation, it could, without	(16a) Where the IICB finds that the Union entities have not applied or implemented this Regulation, including the	

		<p>prejudice to the internal procedures of the Union entity concerned, request relevant and available documentation relating to the effective implementation of the provisions of this Regulation, communicate a reasoned opinion with observed gaps in the implementation of this Regulation, invite the Union entity concerned to provide a self-assessment on its reasoned opinion and issue, in cooperation with CERT-EU, guidance to bring its respective risk management, governance and control framework, cybersecurity risk-management measures, cybersecurity plans and reporting obligations in compliance with this Regulation.</p>	<p>guidance documents, recommendations or calls for action issued under this Regulation, it may, without prejudice to the internal procedures of the relevant Union entity, proceed with compliance measures. The system of compliance measures should be used with a progressive severity, meaning that when the IICB adopts the compliance measures it should start with a warning as the least severe measure and if necessary escalate all the way to the most severe measure of issuing an advisory recommending temporary suspension of data flows to the concerned Union entity, which would be applied in exceptional cases of long-term, deliberate and/or serious non-compliance of the concerned entity with its obligation under this Regulation.</p>	
25b			<p>(16b) The warning represents the least severe compliance measure addressing identified shortcomings of the Union entity and comprising recommendations to amend its</p>	

			cybersecurity documents, in a specified timeframe. The warning should be available to all Union entities, unless restricted appropriately in accordance with this Regulation.	
25c			(16c) The IICB may further recommend an audit of a Union entity be carried out. The Union entity may use its internal audit function for this purpose. The IICB could also request that an audit is carried out by a third-party audit service, including from a mutually agreed private sector service provider.	
25d			(16d) On the basis of the results of an audit carried out upon a recommendation or a request of the IICB, the IICB may further request the Union entity to bring the management, governance, and control of cybersecurity risks into compliance with the provisions of this Regulation.	

25e			<p>(16e) As the Member States share with relevant Union entities information that may be of sensitive nature, the cybersecurity of the addressee of such information is crucial for the Member States. Therefore, in exceptional cases of long-term, deliberate, repetitive and/or serious non-fulfillment of the obligation of the Union entity, the IICB may issue as a last resort measure an advisory to all Member States and Union entities recommending temporary suspension of data flows the Union entity, that should be in place until the state of the cybersecurity of this entity is rectified. This advisory should be communicated to all Member States and Union entities through appropriate secure communication channels.</p>	
25f			<p>(16f) To ensure the correct implementation of this Regulation, the IICB should, if it</p>	

			<p>considers that a continuous breach of this Regulation by a Union entity has been caused directly by the actions or omission of a member of its staff, including at the highest level of management, request the Union entity concerned to take appropriate actions against that staff member, in accordance with the Staff Regulations as well as other equivalent rules applicable in certain Union entities. These actions may include, for instance, disciplinary proceedings and, where appropriate, in the specific case of Union agencies, a request to the competent authority to take the necessary steps related to the possible removal from office of the person that could be responsible for the continuous breach of this Regulation.</p>	
Recital 17				
26	<p>(17) CERT-EU should have the mission to contribute to the security of the IT environment of all Union institutions, bodies and agencies. CERT-EU should act as the equivalent of the designated coordinator for the Union</p>	<p>(17) CERT-EU should have the mission to contribute to the security of the FIICT environment of all Union institutions, bodies and agencies entities. Where appropriate, and in coordination with the Union entities, CERT-</p>	<p>(17) CERT-EU should have the mission to contribute to the security of the IT environment of all Union entities. When considering whether to provide technical advice or input on relevant policy matters upon the</p>	

	<p>institutions, bodies and agencies, for the purpose of coordinated vulnerability disclosure to the European vulnerability registry as referred to in Article 6 of Directive [proposal NIS 2].</p>	<p>EU may submit to the IICB for its approval, a proposal for a coordinated cyber insurance policy covering Union entities, in order to establish first and third-party coverage to address the potential impact of incidents. CERT-EU should act as the equivalent of the designated coordinator for the Union institutions, bodies and agencies entities, for the purpose of coordinated vulnerability disclosure to the European vulnerability registry database as referred to in Article 612 of Directive [proposal NIS 2](EU) 2022/2555.</p>	<p>request of a Union entity, CERT-EU should ensure that this does not impede the fulfilment of its other tasks laid down in this Regulation institutions, bodies and agencies. CERT-EU should act as the equivalent of the designated coordinator for the Union institutions, bodies and agencies, for the purpose of coordinated vulnerability disclosure to the European vulnerability registry as referred to in Article 6 of Directive [proposal NIS 2].</p>	
26a			<p>(17a) CERT-EU should act as the equivalent of the designated coordinator for the Union entities, for the purpose of coordinated vulnerability disclosure to the European vulnerability registry as referred to in Article 6 of Directive [proposal NIS 2] and should develop a policy on management of vulnerabilities, encompassing the promotion and facilitation of voluntary coordinated</p>	

			vulnerability disclosure.	
Recital 18				
27	(18) In 2020, CERT-EU's Steering Board set a new strategic aim for CERT-EU to guarantee a comprehensive level of cyber defence for all Union institutions, bodies and agencies with suitable breadth and depth and continuous adaptation to current or impending threats, including attacks against mobile devices, cloud environments and internet-of-things devices. The strategic aim also includes broad-spectrum Security Operations Centres (SOCs) that monitor networks, and 24/7 monitoring for high-severity threats. For the larger Union institutions, bodies and agencies, CERT-EU should support their IT security teams, including with first-line 24/7 monitoring. For smaller and some medium-sized Union institutions, bodies and agencies, CERT-EU should provide all the services.	(18) In 2020, CERT-EU's Steering Board set a new strategic aim for CERT-EU to guarantee a comprehensive level of cyber defence for all Union institutions, bodies and agencies entities with suitable breadth and depth and continuous adaptation to current or impending threats, including attacks against mobile devices, cloud environments and internet-of-things devices. The strategic aim also includes broad-spectrum Security Operations Centres (SOCs) that monitor networks, and 24/7 monitoring for high-severity threats. For the larger Union institutions, bodies and agencies entities , CERT-EU should support their IT FI CT security teams, including with first-line 24/7 monitoring. For smaller and some medium-sized Union institutions, bodies and agencies entities , CERT-EU should provide all the services.	<i>deleted</i>	
Recital 19				
28	(19) CERT-EU should also fulfil	(19) CERT-EU should also fulfil	(19) CERT-EU should also	

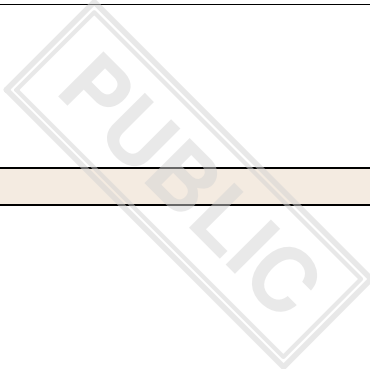
	<p>the role provided for it in Directive [proposal NIS 2] concerning cooperation and information exchange with the computer security incident response teams (CSIRTs) network. Moreover, in line with Commission Recommendation (EU) 2017/1584¹, CERT-EU should cooperate and coordinate on the response with the relevant stakeholders. In order to contribute to a high level of cybersecurity across the Union, CERT-EU should share incident specific information with national counterparts. CERT-EU should also collaborate with other public as well as private counterparts, including at NATO, subject to prior approval by the IICB.</p> <p>¹ Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).</p>	<p>the role provided for it in Directive [proposal NIS 2] (EU) 2022/2555 concerning cooperation and information exchange with the computer security incident response teams (CSIRTs) network. Moreover, in line with Commission Recommendation (EU) 2017/1584¹, CERT-EU should cooperate and coordinate on the response with the relevant stakeholders. In order to contribute to a high level of cybersecurity across the Union, CERT-EU should share incident specific information with national counterparts. CERT-EU should also collaborate with other public as well as private counterparts, including at NATO, subject to prior approval by the IICB.</p> <p>¹ Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).</p>	<p>fulfill fulfill the role provided for it in Directive [proposal NIS 2] concerning cooperation and information exchange with the computer security incident response teams (CSIRTs) network. Moreover, in line with Commission Recommendation (EU) 2017/1584^{1,2}, CERT-EU should cooperate and coordinate on the response with the relevant stakeholders. In order to contribute to a high level of cybersecurity across the Union, CERT-EU should share incident specific information with national counterparts. CERT-EU should also collaborate with other public as well as private counterparts, including at NATO, subject to prior approval by the IICB.</p> <p>¹ Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).</p> <p>² Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).</p>	
Recital 20				
29	(20) In supporting operational	(20) In supporting operational	(20) In supporting operational	

	<p>cybersecurity, CERT-EU should make use of the available expertise of the European Union Agency for Cybersecurity through structured cooperation as provided for in Regulation (EU) 2019/881 of the European Parliament and of the Council¹. Where appropriate, dedicated arrangements between the two entities should be established to define the practical implementation of such cooperation and to avoid the duplication of activities. CERT-EU should cooperate with the European Union Agency for Cybersecurity on threat analysis and share its threat landscape report with the Agency on a regular basis.</p> <p>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).</p>	<p>cybersecurity, CERT-EU should make use of the available expertise of the European Union Agency for Cybersecurity (ENISA) through structured cooperation as provided for in Regulation (EU) 2019/881 of the European Parliament and of the Council¹. Where appropriate, Dedicated arrangements between the two entities should be established within two years of the date of entry into force of this Regulation, to define the practical implementation of such cooperation and to avoid the duplication of activities. CERT-EU should cooperate with the European Union Agency for Cybersecurity ENISA on threat analysis and share its threat landscape report with the Agency on a regular basis.</p> <p>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).</p>	<p>cybersecurity, CERT-EU should make use of the available expertise of the European Union Agency for Cybersecurity (ENISA) through structured cooperation as provided for in Regulation (EU) 2019/881 of the European Parliament and of the Council¹³. Where appropriate, dedicated arrangements between the two entities should be established to define the practical implementation of such cooperation and to avoid the duplication of activities. CERT-EU should cooperate with the European Union Agency for Cybersecurity ENISA on threat analysis and share its threat landscape report with the Agency on a regular basis.</p> <p>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).</p> <p>3. 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</p>	
--	--	--	--	--

			(Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).	
Recital 21				
30	<p>(21) In support of the Joint Cyber Unit built in accordance with the Commission Recommendation of 23 June 2021¹, CERT-EU should cooperate and exchange information with stakeholders to foster operational cooperation and to enable the existing networks in realising their full potential in protecting the Union.</p> <p>¹ Commission Recommendation C(2021) 4520 of 23.6.2021 on building a Joint Cyber Unit.</p>	<p>(21) In support of the Joint Cyber Unit built in accordance with the Commission Recommendation of 23 June 2021¹, CERT-EU should cooperate and exchange information with stakeholders to foster operational cooperation and to enable the existing networks in realising their full potential in protecting the Union.</p> <p>¹ Commission Recommendation C(2021) 4520 of 23.6.2021 on building a Joint Cyber Unit.</p>	<i>deleted</i>	
Recital 22				
31	<p>(22) All personal data processed under this Regulation should be processed in accordance with data protection legislation including Regulation (EU) 2018/1725 of the European Parliament and of the Council.¹</p> <p>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</p>	<p>(22) All personal data processed under this Regulation should be processed in accordance with data protection legislationlaw including Regulation (EU) 2018/1725 of the European Parliament and of the Council¹.⁺ This Regulation should not affect the application of Union law governing the processing of personal data, including the tasks conferred on and powers of the European</p>	<p>(22) The activities and information handling of CERT-EU under this Regulation may involve processing of personal data. All personal data processed under this Regulation should be processed in accordance with data protection legislation including Regulation (EU) 2018/1725 of the European Parliament and of the Council⁴.⁺ Where pursuant to this Regulation personal data is</p>	

	<p>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).</p>	<p>Data Protection Supervisor (EDPS). CERT-EU and the IICB should work in close cooperation with the EPDS and the staff specialised in data protection in the Union entities to ensure full compliance with Union data protection law.</p> <p>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, p. 39).</p>	<p>transmitted to recipients established in the Union other than Union entities, this should be done in accordance with Article 9 of Regulation (EU) 2018/1725.</p> <p>4. 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, p. 39).</p> <p>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, p. 39).</p>	
31a		<p>(22a) Cybersecurity systems and services involved in the prevention, detection and response to cyber threats should comply with data protection and privacy law and should take relevant technical and organisational safeguarding</p>		

		measures to ensure that such compliance is achieved in an accountable way.		
31b		<p>(22b) Open-source cybersecurity tools and applications can contribute to a higher degree of openness. Open standards facilitate interoperability between security tools, benefitting the security of stakeholders. Open-source cybersecurity tools and applications can leverage the wider developer community, enabling diversification of suppliers. Open source can lead to a more transparent verification process of cybersecurity related tools and a community-driven process of discovering vulnerabilities. Union entities should therefore be able to promote the use of open-source software and open standards by pursuing policies relating to the use of open data and open-source as part of security through transparency.</p>		
Recital 23				



32	<p>(23) The handling of information by CERT-EU and the Union institutions, bodies and agencies should be in line with the rules laid down in Regulation [proposed Regulation on information security]. To ensure coordination on security matters, any contacts with CERT-EU initiated or sought by national security and intelligence services should be communicated to the Commission's Security Directorate and the chair of the IICB without undue delay.</p>	<p>(23) The handling of information by CERT-EU and the Union institutions, bodies and agenciesentities should be in line with the rules on information security, in particular those laid down in Regulation [proposed Regulation on information security]. To ensure coordination on security matters, any contacts with CERT-EU initiated or sought by national security and intelligence services should be communicated to the Commission's Security Directorate and the chair of the IICB without undue delay.</p>	<p>(23) The handling of information by CERT-EU and the Union institutions, bodies and agenciesUnion entities should be in line with the rules laid down in Regulation [proposed Regulationapplicable rules on information security]. To ensure coordination on security matters, any contacts with CERT-EU initiated or sought by national security and intelligence services should be communicated to the Commission's Security Directorate and the chair of the IICB without undue delay.</p>	
32a			<p>(23a) For the purposes of sharing information visible markings are used to indicate that sharing boundaries are to be applied by the recipients of the information based on, in particular, non-disclosure agreements, or informal non-disclosure agreements such as the traffic light protocol or other clear indications by the source. The traffic light protocol is to be understood as a means to</p>	

			<p>provide information about any limitations with regard to the further spreading of information. It is used in almost all computer security incident response teams (CSIRTs) and in some information analysis and sharing centres.</p>	
Recital 24				
33	<p>(24) As the services and tasks of CERT-EU are in the interest of all Union institutions, bodies and agencies, each Union institution, body and agency with IT expenditure should contribute a fair share to those services and tasks. Those contributions are without prejudice to the budgetary autonomy of the Union institutions, bodies and agencies.</p>	<p>(24) As the services and tasks of CERT-EU are in the interest of all Union institutions, bodies and agenciesentities, each Union institution, body and agency with ITentity with ICT expenditure should contribute a fair share to those services and tasks. Those contributions are without prejudice to the budgetary autonomy of the Union institutions, bodies and agenciesentities.</p>	<p>(24) This Regulation and the new tasks allocated to CERT-EU will have no effect on the total expenditures under the Multiannual Financial Framework. As the services and tasks of CERT-EU are in the interest of all Union institutions, bodies and agenciesentities, each Union institution, body and agencyentity with IT expenditure should contribute a fair share to those services and tasks. Those contributions are without prejudice to the budgetary autonomy of the Union institutions, bodies and agenciesentities. All Union entities and their administrations should ensure the optimisation of their resources at the current level and strengthen efficiency gains including by deepening inter-institutional cooperation in</p>	

			<p>the area of cybersecurity. Therefore, a joint approach to pooling administrative expenditure should be given preference over individualised spending of Union entities.</p>	
Recital 25				
33a		<p><i>(24a) This Regulation should take into account the fact that, apart from the Union institutions, most of Union entities, in particular the small ones, do not have the necessary financial and human resources to be dedicated for additional cybersecurity tasks.</i></p>		
Recital 25				
34	<p>(25) The IICB, with the assistance of CERT-EU, should review and evaluate the implementation of this Regulation and should report its findings to the Commission. Building on this input, the Commission should report to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.</p>	<p>(25) The IICB, with the assistance of CERT-EU, should review and evaluate the implementation of this Regulation and should report its findings to the Commission. Building on this input, the Commission should report to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.</p>	<p>(25) The IICB, with the assistance of CERT-EU, should review and evaluate the implementation of this Regulation and should report its findings to the Commission. Building on this input, the Commission should report to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Furthermore, the European Court of Auditors is invited to evaluate the</p>	

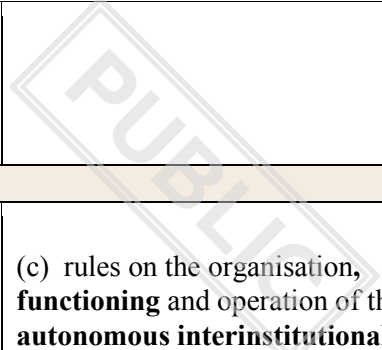
			functioning of CERT-EU on a regular basis.	
--	--	--	---	--

PUBLIC



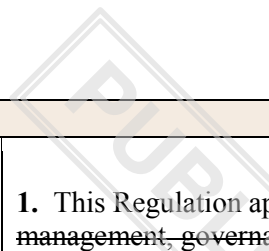
Formula				
35	HAVE ADOPTED THIS REGULATION:	HAVE ADOPTED THIS REGULATION:	HAVE ADOPTED THIS REGULATION:	HAVE ADOPTED THIS REGULATION: <small>Text Origin: Commission Proposal</small>
Chapter I				
36	Chapter I GENERAL PROVISIONS	Chapter I GENERAL PROVISIONS	Chapter I GENERAL PROVISIONS	Chapter I GENERAL PROVISIONS <small>Text Origin: Commission Proposal</small>
Article 1				
37	Article 1 Subject-matter	Article 1 Subject-matter	Article 1 Subject-matter	Article 1 Subject-matter <small>Text Origin: Commission Proposal</small>
Article 1, first paragraph				
38	This Regulation lays down:	This Regulation lays down measures that aim to achieve a high common level of cybersecurity in Union entities.	This Regulation lays down- measures that aim to achieve a high common level of cybersecurity within Union	This Regulation lays down- <u>measures that aim to achieve a high common level of cybersecurity within Union</u>

		To that end, this Regulation lays down:	entities	<u>entities</u> Text Origin: Council Mandate
Article 1, first paragraph, point (a)				
G	39	(a) obligations on Union institutions, bodies and agencies to establish an internal cybersecurity risk management, governance and control framework;	(a) obligations on Union institutions, bodies and agencies that require Union entities to establish an internal cybersecurity risk management, handling of incidents , governance and control framework;	(a) obligations on Union institutions, bodies and agencies each Union entity to establish an internal a cybersecurity risk management, governance and control framework; linked to handling of incidents later in the articles. line 63 change to 'entities' agreed Text Origin: Council Mandate
Article 1, first paragraph, point (b)				
Y	40	(b) cybersecurity risk management and reporting obligations for Union institutions, bodies and agencies;	(b) cybersecurity risk management and reporting obligations for Union institutions, bodies and agencies entities ;	and, reporting and information sharing obligations for Union institutions, bodies and agencies entities ; align with art 19
Article 1, first paragraph, point (ba)				
Y	40a		(ba) rules underpinning information sharing obligations and the facilitation of voluntary	align with art 19



		information sharing arrangements with regard to Union entities;		
Article 1, first paragraph, point (c)				
41	(c) rules on the organisation and operation of the Cybersecurity Centre for the Union institutions, bodies and agencies (CERT-EU) and on the organisation and operation of the Interinstitutional Cybersecurity Board.	(c) rules on the organisation, tasks and operation of the Cybersecurity Centre for the Union institutions, bodies and agencies entities (CERT-EU) and on the functioning , organisation and operation of the Interinstitutional Cybersecurity Board (IICB).	(c) rules on the organisation, functioning and operation of the autonomous interinstitutional computer emergency response team -Cybersecurity Centre for the Union institutions, bodies and agencies entities (CERT-EU) and on the organisation, functioning and operation of the Interinstitutional Cybersecurity Board: (IICB);	
Article 1, first paragraph, point (d)				
41a			(d) rules relating to the monitoring of the implementation of this Regulation.	lawyer linguists to propose different formulation for rules. in principle ok for EP
Article 2				
42	Article 2 Scope	Article 2 Scope	Article 2 Scope	Article 2 Scope Text Origin: Commission Proposal

PUBLIC



Article 2, first paragraph

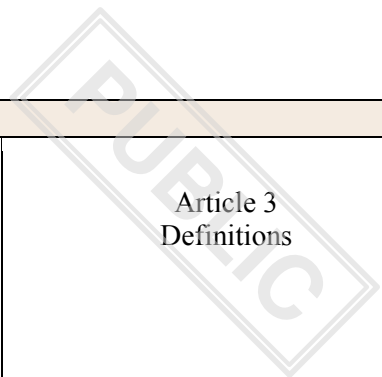
Y	43	This Regulation applies to the management, governance and control of cybersecurity risks by all Union institutions, bodies and agencies and to the organisation and operation of CERT-EU and the Interinstitutional Cybersecurity Board.	This Regulation applies to the management, governance and control of cybersecurity risks by all Union institutions, bodies and agencies entities and to the functioning , organisation and operation of CERT-EU and the Interinstitutional Cybersecurity Board IICB .	1. This Regulation applies to the management, governance and control of cybersecurity risks by all Union institutions, bodies and agencies entities and to the organisation and operation of CERT-EU and the Interinstitutional Cybersecurity Board IICB .	linked to chapter IV on functioning of CERT-EU	Y
---	----	--	---	--	--	---

Article 2, second paragraph

G	43a			2. This Regulation applies without prejudice to the institutional autonomy pursuant to the Treaties.	<u>2. This Regulation applies without prejudice to the institutional autonomy pursuant to the Treaties.</u> Text Origin: Council Mandate	G
---	-----	--	--	--	---	---

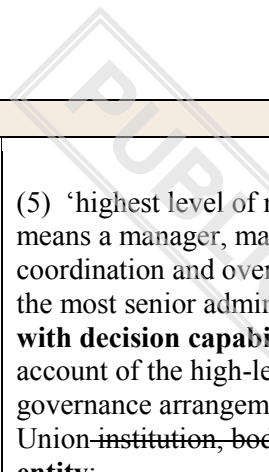
Article 2, third paragraph

Y	43b			3. With the exception of Article 12(7), this Regulation shall not apply to network and information systems handling EU Classified Information (EUCI).	EP to check	Y
---	-----	--	--	---	-------------	---



Article 3				
44	Article 3 Definitions	Article 3 Definitions	Article 3 Definitions	Article 3 Definitions Text Origin: Commission Proposal
Article 3, first paragraph				
45	For the purpose of this Regulation, the following definitions apply:	For the purpose of this Regulation, the following definitions apply:	For the purpose of this Regulation, the following definitions apply:	For the purpose of this Regulation, the following definitions apply: Text Origin: Commission Proposal
Article 3, first paragraph, point (1)				
46	(1) 'Union institutions, bodies and agencies' means the Union institutions, bodies and agencies set up by, or on the basis of, the Treaty on European Union, the Treaty on the functioning of European Union or the Treaty establishing the European Atomic Energy Community;	(1) 'Union institutions, bodies and agencies entities ' means the Union institutions, bodies, offices and agencies set up by, or on the basis of, the Treaty on European Union, the Treaty on the functioning of European Union or the Treaty establishing the European Atomic Energy Community;	(1) 'Union institutions, bodies and agencies entities ' means the Union institutions, bodies, offices and agencies set up by, or on the basis of, the Treaty on European Union, the Treaty on the functioning of European Union or the Treaty establishing the European Atomic Energy Community;	(1) 'Union institutions, bodies and agencies entities ' means the Union institutions, bodies, offices and agencies set up by, or on the basis of, the Treaty on European Union, the Treaty on the functioning of European Union or the Treaty establishing the European Atomic Energy Community;
Article 3, first paragraph, point (2)				
47				

	(2) ‘network and information system’ means network and information system within the meaning of Article 4(1) of Directive [proposal NIS 2];	(2) ‘network and information system’ means network and information system within the meaning of Article 4(1) as defined in Article 6, point (1), of Directive [proposal NIS 2](EU) 2022/2555;	(2) ‘network and information system’ means a network and information system within the meaning of as defined in Article 4(1) of Directive [proposal NIS 2];	(2) ‘network and information system’ means <u>a</u> network and information system within the meaning of as defined in Article 4(1) 6, point (1), of Directive [proposal NIS 2](EU) 2022/2555; Text Origin: EP Mandate
Article 3, first paragraph, point (3)				
48	(3) ‘security of network and information systems’ means security of network and information systems within the meaning of Article 4(2) of Directive [proposal NIS 2];	(3) ‘security of network and information systems’ means security of network and information systems within the meaning of Article 4(2) as defined in Article 6, point (2), of Directive [proposal NIS 2](EU) 2022/2555;	(3) ‘security of network and information systems’ means security of network and information systems within the meaning of as defined in Article 4(2) of Directive [proposal NIS 2];	(3) ‘security of network and information systems’ means security of network and information systems within the meaning of Article 4(2) as defined in Article 6, point (2), of Directive [proposal NIS 2](EU) 2022/2555; Text Origin: EP Mandate
Article 3, first paragraph, point (4)				
49	(4) ‘cybersecurity’ means cybersecurity within the meaning of Article 4(3) of Directive [proposal NIS 2];	(4) ‘cybersecurity’ means cybersecurity within the meaning of Article 4(3) of Directive [proposal NIS 2] as defined in Article 2, point (1), of Regulation (EU) 2019/881;	(4) ‘cybersecurity’ means cybersecurity as defined in Article 2, point (1), of Regulation (EU) 2019/881 within the meaning of Article 4(3) of Directive [proposal NIS 2];	(4) ‘cybersecurity’ means cybersecurity within the meaning of Article 4(3) of Directive [proposal NIS 2] as defined in Article 2, point (1), of Regulation (EU) 2019/881; Text Origin: EP Mandate



Article 3, first paragraph, point (5)

50	(5) ‘highest level of management’ means a manager, management or coordination and oversight body at the most senior administrative level, taking account of the high-level governance arrangements in each Union institution, body or agency;	(5) ‘highest level of management’ means a manager, management or coordination and oversight body responsible for the functioning of the Union entity concerned , at the most senior administrative level, taking account of with a mandate to adopt or authorise decisions in line with the high-level governance arrangements in each Union institution, body or agency of the entity concerned, without prejudice to the formal responsibilities of other levels of management for compliance and risk management in their respective areas of responsibility;	(5) ‘highest level of management’ means a manager, management or coordination and oversight body at the most senior administrative level with decision capabilities , taking account of the high-level governance arrangements in each Union institution, body or agency entity;	Council to check if EP text ok
----	---	---	---	--------------------------------

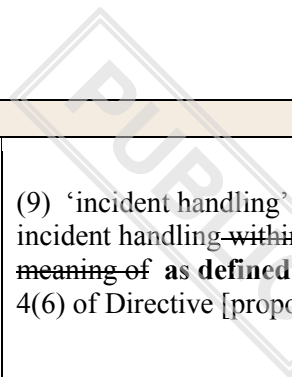
Article 3, first paragraph, point (5a)

50a		(5a) 'near miss' means a near miss as defined in Article 6, point (5), of Directive (EU) 2022/2555;	(5a) ‘near miss’ means a near miss as defined in Article 4(4a) of Directive [proposal NIS 2];	<u>(5a) 'near miss' means a near miss as defined in Article 6, point (5), of Directive (EU) 2022/2555;</u> Text Origin: EP Mandate
-----	--	---	---	---

Article 3, first paragraph, point (6)

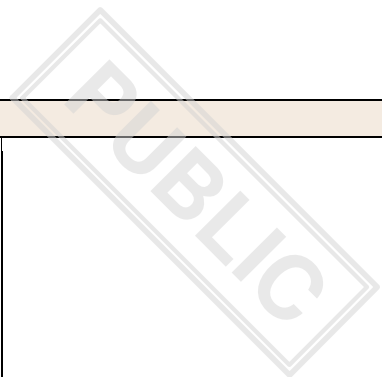
51	(6) ‘incident’ means an incident	(6) ‘incident’ means an incident	(6) ‘incident’ means an incident	(6) ‘incident’ means an incident
----	----------------------------------	----------------------------------	----------------------------------	----------------------------------

	within the meaning of Article 4(5) of Directive [proposal NIS 2];	within the meaning of Article 4(5) as defined in Article 6, point (6) , of Directive [proposal NIS 2] (EU) 2022/2555;	within the meaning of as defined in Article 4(5) of Directive [proposal NIS 2];	within the meaning of Article 4(5) as defined in Article 6, point (6) , of Directive [proposal NIS 2] (EU) 2022/2555; Text Origin: EP Mandate
Article 3, first paragraph, point (7)				
52	(7) ‘significant incident’ means any incident unless it has limited impact and is likely to be already well understood in terms of method or technology;	<i>deleted</i>	<i>deleted</i>	(7) <i>‘significant incident’ means any incident unless it has limited impact and is likely to be already well understood in terms of method or technology;</i> deleted
Article 3, first paragraph, point (8)				
53	(8) ‘major attack’ means any incident requiring more resources than are available at the affected Union institution, body or agency and at CERT-EU;	(8) ‘major attack incident ’ means any an incident requiring more resources than are available at the affected whose disruption exceeds an affected Union entity’s and CERT-EU’s capacity to respond to it, or which has a significant impact on at least two Union institution, body or agency and at CERT-EU entities, or where a large-scale cybersecurity incident as defined in Article 6, point (7), of Directive (EU) 2022/2555 has a significant impact on at least one Union entity;	(8) ‘major attack incident ’ means any incident requiring more resources than are available at the affected which causes a level of disruption that exceeds a Union institution, body or agency and at CERT-EU entity’s and CERT-EU’s capacity to respond to it or which has a significant impact on at least two Union entities;	(8) ‘major attack incident ’ means any incident requiring more resources than are available at the affected which causes a level of disruption that exceeds a Union institution, body or agency and at CERT-EU entities, for where a large-scale cybersecurity incident as defined in Article 6, point (7), of Directive (EU) 2022/2555 has a significant impact on at least one Union entity; to be discussed with art 12

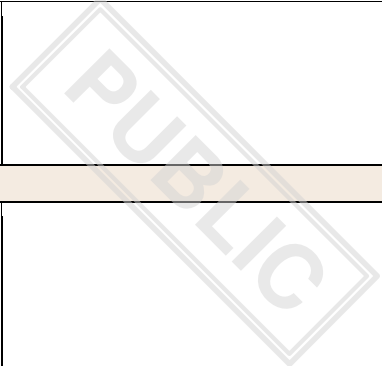


Article 3, first paragraph, point (9)				
54	(9) ‘incident handling’ means incident handling within the meaning of Article 4(6) of Directive [proposal NIS 2];	(9) ‘incident handling’ means incident handling within the meaning of Article 4(6) as defined in Article 6, point (8), of Directive [proposal NIS 2] (EU) 2022/2555;	(9) ‘incident handling’ means incident handling within the meaning of as defined in Article 4(6) of Directive [proposal NIS 2];	(9) ‘incident handling’ means incident handling within the meaning of Article 4(6) as defined in Article 6, point (8), of Directive [proposal NIS 2] (EU) 2022/2555; Text Origin: EP Mandate
Article 3, first paragraph, point (10)				
55	(10) ‘cyber threat’ means cyber threat within the meaning of Article 2(8) of Regulation (EU) 2019/881;	(10) ‘cyber threat’ means cyber threat within the meaning of as defined in Article 2(8)2, point (8), of Regulation (EU) 2019/881;	(10) ‘cyber threat’ means cyber threat within the meaning of as defined in Article 2(8) of Regulation (EU) 2019/881;	(10) ‘cyber threat’ means cyber threat within the meaning of as defined in Article 2(8)2, point (8), of Regulation (EU) 2019/881; Text Origin: EP Mandate
Article 3, first paragraph, point (11)				
56	(11) ‘significant cyber threat’ means a cyber threat with the intention, opportunity and capability to cause a significant incident;	(11) ‘significant cyber threat’ means a cyber threat with the intention, opportunity and capability to cause a significant incident as defined in Article 6, point (11), of Directive (EU) 2022/2555;	<i>deleted</i>	<i>linked to art 20 (1) [Council]</i>

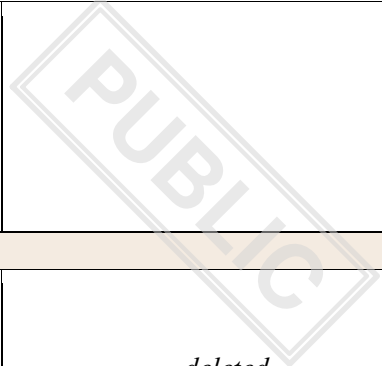
Article 3, first paragraph, point (12)				
57	(12) ‘vulnerability’ means vulnerability within the meaning of Article 4(8) of Directive [proposal NIS 2];	(12) ‘vulnerability’ means vulnerability within the meaning of as defined in Article 4(8)6, point (15), of Directive [proposal NIS 2](EU) 2022/2555;	(12) ‘vulnerability’ means vulnerability within the meaning of Article 4(8) of Directive [proposal NIS 2];	(12) ‘vulnerability’ means vulnerability within the meaning of as defined in Article 4(8)6, point (15), of Directive [proposal NIS 2](EU) 2022/2555; Text Origin: EP Mandate
Article 3, first paragraph, point (13)				
58	(13) ‘significant vulnerability’ means a vulnerability that will likely lead to a significant incident if it is exploited;	(13) ‘significant vulnerability’ means a vulnerability that will likely lead to a significant incident if it is exploited;	<i>deleted</i>	<i>linked to article 20</i>
Article 3, first paragraph, point (14)				
59	(14) ‘cybersecurity risk’ means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems;	(14) ‘ cybersecurity -risk’ means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems a risk as defined in Article 6, point (9), of Directive (EU) 2022/2555;	(14) ‘ cybersecurity risk’ means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems a risk within the meaning of Article 4(7b) of Directive [proposal NIS 2] ;	(14) ‘ cybersecurity -risk’ means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems a risk as defined in Article 6, point (9), of Directive (EU) 2022/2555; Text Origin: EP Mandate



Article 3, first paragraph, point (14a)				
59a		<p>(14a) ‘standard’ means a standard as defined in Article 2, point (1), of Regulation (EU) No 1025/2012 of the European Parliament and of the Council¹;</p> <p>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).</p>		Council to check
Article 3, first paragraph, point (14b)				
59b		<p>(14b) ‘technical specification’ means a technical specification as defined in Article 2, point (4), of Regulation (EU) No 1025/2012;</p>		not retained
Article 3, first paragraph, point (14c)				
59c		<p>(14c) ‘ICT product’ means an</p>		



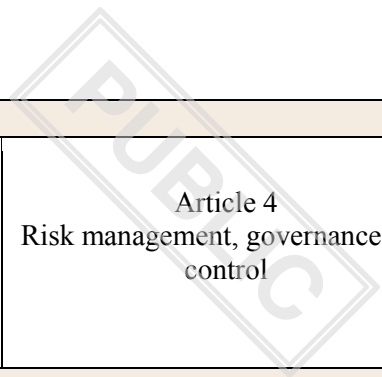
		ICT product as defined in of Article 2, point (12), of Regulation (EU) 2019/881;		
Y	59d	(14d) ‘ICT service’ means an ICT service as defined in Article 2, point (13), of Regulation (EU) 2019/881;		Y
Y	59e	(14e) ‘ICT process’ means an ICT process as defined in Article 2, point (14), of Regulation (EU) 2019/881;		Y
	Article 3, first paragraph, point (14c)			
Y	59f	(14f) ‘ICT environment’ means any on-premise or virtual ICT product, ICT service and ICT process, any network and information system, whether owned and operated by a entity, or hosted or operated by a third party, including mobile devices, corporate networks, and business networks not connected to the internet and any devices connected to the ICT		Y
			EC to propose new drafting	



		environment and any dislocated premises and decentralised offices, such as liaison offices, representative offices or local offices;			
Article 3, first paragraph, point (15)					
R	60	(15) ‘Joint Cyber Unit’ means a virtual and physical platform for cooperation for the different cybersecurity communities in the Union, with a focus on operational and technical coordination against major cross-border cyber threats and incidents within the meaning of Commission Recommendation of 23 June 2021;	(15) ‘Joint Cyber Unit’ means a virtual and physical platform for cooperation for the different cybersecurity communities in the Union, with a focus on operational and technical coordination against major cross-border cyber threats and incidents within the meaning of Commission Recommendation of 23 June 2021;	deleted	legal services to discuss possibly for trilogue agenda
Article 3, first paragraph, point (16)					
Y	61	(16) ‘cybersecurity baseline’ means a set of minimum cybersecurity rules with which network and information systems and their operators and users must be compliant, to minimise cybersecurity risks.	(16) ‘cybersecurity baseline measures ’ means a set of minimum cybersecurity rules and measures with which network and information systems and their operators and users must be compliant, to minimise cybersecurity risks.	deleted	to be discussed with art 5
Article 3, first paragraph, point (16a)					
	61a				

			Article 3a Processing of personal data	discuss together with art 18
Article 3a, (1)				
61b			1. The processing of personal data under this Regulation by CERT-EU, the IICB or Union entities shall be carried out in compliance with Regulation (EU) 2018/1725.	
Article 3a (2)				
61c			2. CERT-EU, the IICB and Union entities shall process and exchange personal data to the extent necessary and for the sole purpose of fulfilling their respective obligations under this Regulation.	
Chapter II				
62	Chapter II MEASURES FOR A HIGH COMMON LEVEL OF CYBERSECURITY	Chapter II MEASURES FOR A HIGH COMMON LEVEL OF CYBERSECURITY	Chapter II MEASURES FOR A HIGH COMMON LEVEL OF CYBERSECURITY	Chapter II MEASURES FOR A HIGH COMMON LEVEL OF CYBERSECURITY Text Origin: Commission Proposal

PUBLIC



Article 4

63	Article 4 Risk management, governance and control	Article 4 Risk management, handling of incidents , governance and control framework	Article 4 Risk management, governance and control	Article 4 Risk management, governance and control <u>framework</u>
----	--	--	--	---

Article 4(1)

64	<p>1. Each Union institution, body and agency shall establish its own internal cybersecurity risk management, governance and control framework ('the framework') in support of the entity's mission and exercising its institutional autonomy. This work shall be overseen by the entity's highest level of management to ensure an effective and prudent management of all cybersecurity risks. The framework shall be in place by at the latest [15 months after the entry into force of this Regulation].</p>	<p>1. Each Union institution, body and agency On the basis of a full cybersecurity audit, each Union entity shall establish its own internal cybersecurity risk management, handling of incidents, governance and control framework ('the framework') in support of the Union entity's mission and exercising its institutional autonomy. This work The establishment of the framework shall be overseen by the Union entity's highest level of management and shall be under its responsibility in order to ensure an effective and prudent management of all cybersecurity risks. The framework shall be in place by at the latest established by ... [15 months after the date of entry into force of</p>	<p>1. Each Union institution, body and agency entity shall establish its own internal cybersecurity risk management, governance and control framework ('the framework') in support of the entity's mission and exercising its institutional autonomy. The framework This work shall be overseen by the entity's highest level of management to ensure an effective and prudent management of all cybersecurity risks. The framework shall be in place by at the latest [15 months after the entry into force of this Regulation].</p>	<p>EC to suggest new drafting</p>
----	---	---	---	-----------------------------------

		this Regulation].		
Article 4(2)				
65	<p>2. The framework shall cover the entirety of the IT environment of the concerned institution, body or agency, including any on-premise IT environment, outsourced assets and services in cloud computing environments or hosted by third parties, mobile devices, corporate networks, business networks not connected to the internet and any devices connected to the IT environment. The framework shall take account of business continuity and crisis management and it shall consider supply chain security as well as the management of human risks that could impact the cybersecurity of the concerned Union institution, body or agency.</p>	<p>2. The framework shall cover the entirety of the IT ICT environment of the concerned institution, body or agency, including any on-premise IT environment, outsourced assets and services in cloud computing environments or hosted by third parties, mobile devices, corporate networks, business networks not connected to the internet and any devices connected to the IT environment Union entity concerned. The framework shall take account of business continuity and crisis management and it shall consider supply chain security as well as the management of human risks and all other relevant technical, operational and organisational risks that could have an impact on the cybersecurity of the concerned Union institution, body or agency entity concerned.</p>	<p>2. The framework shall cover the entirety of the unclassified IT environment of the concerned institution, body or agency Union entity, including any on-premise IT environment, operational technology network, outsourced assets and services in cloud computing environments or hosted by third parties, mobile devices, corporate networks, business networks not connected to the internet and any devices connected to the IT environment. The framework shall take account of business continuity and crisis management and it shall consider supply chain security as well as the management of human be based on an all-hazard approach and on a maturity assessment in accordance with Article 6 covering all the relevant technical, operational and organisational risks that could impact the cybersecurity of the concerned Union institution, body or agency entity .</p>	To be discussed as a political point
Article 4(2a)				

65a		<p>2a. The framework referred to in paragraph 1 shall define strategic objectives to ensure a high level of cybersecurity in the Union entities. That framework shall lay down cybersecurity policies for the security of network and information systems encompassing the entirety of the ICT environment, and define the roles and responsibilities of staff of the Union entities tasked with ensuring the effective implementation of this Regulation. The framework shall also include the key performance indicators (KPIs) for measuring the effectiveness of the implementation based on the KPIs list referred to in Article 12(2), point (eb).</p>	<p>2a. The framework shall lay down cybersecurity policies, including objectives and priorities for the security of network and information systems, and policies and procedures to assess the effectiveness of implemented cybersecurity risk management measures and define staff members' roles and responsibilities.</p>	<p><u>2a. The framework referred to in paragraph 1 shall define strategic objectives to ensure a high level of cybersecurity in the Union entities. That framework shall lay down cybersecurity policies for the security of network and information systems encompassing the entirety of the ICT environment, and define the roles and responsibilities of staff of the Union entities tasked with ensuring the effective implementation of this Regulation. The framework shall also include mechanisms to measure the effectiveness of the implementation, such as those listed in Article 12(2), point (eb)</u></p> <p>Council to reflect, linked to 133b and a recital expanding on KPIs</p> <p>Text Origin: EP Mandate</p>
Article 4(2b)				
65b		<p>2b. The framework referred to in paragraph 1 shall be reviewed on a regular basis and at least every three years. The first such review shall be carried out by ... [three years after the date of</p>	<p>2b. The framework shall be reviewed on a regular basis, and at least every three years in light of the changing risks, the assets and the maturity of the Union entity.</p>	<p><u>2b. The framework referred to in paragraph 1 shall be reviewed on a regular basis and at least every three years. The first such review shall be carried out by ... [51 months after the date of entry into</u></p>



entry into force of this Regulation]. Where appropriate and upon request of the IICB, a Union entity's framework shall be updated following guidance from CERT-EU on incidents identified or possible gaps observed in the implementation of this Regulation.

force of this Regulation]. Where appropriate and upon request of the IICB, a Union entity's framework may be updated following guidance from CERT-EU on incidents identified or possible gaps observed in the implementation of this Regulation.

Council checks with MS

Text Origin: EP Mandate

Article 4(3)

66

3. The highest level of management of each Union institution, body and agency shall provide oversight over the compliance of their organisation with the obligations related to cybersecurity risk management, governance, and control, without prejudice to the formal responsibilities of other levels of management for compliance and risk management in their respective areas of responsibility.

3. The highest level of management of each Union ~~institution, body and agency shall provide oversight over~~ **entity shall be responsible for the implementation and shall oversee** the compliance **and functioning of its** ~~of their~~ organisation with the obligations related to ~~cybersecurity risk management, governance, and control~~ **the framework**, without prejudice to the formal responsibilities of other levels of management for compliance and risk management in their respective areas of responsibility, **such as data protection.**

3. The highest level of management of each Union ~~institution, body and agency~~ **entity** shall ~~provide oversight over~~ **oversee** the compliance of ~~their~~ **its** organisation with the obligations related to cybersecurity risk management, governance, and control, without prejudice to the formal responsibilities of other levels of management for compliance and risk management in their respective areas of responsibility.

Council to check EP text. Linked to row 50

Article 4(3a)			
66a			<p>3a. Where appropriate and without prejudice to its responsibility for the implementation of this Regulation, the highest level of management of each Union entity may delegate to other senior officials within the entity concerned specific obligation under this Regulation. Regardless of possible delegation of its specific obligation, the highest level of management may be held liable for the non-compliance by the entities with the obligations under this Regulation.</p> <p><i><u>3a. Where appropriate and without prejudice to its responsibility for the implementation of this Regulation, the highest level of management of each Union entity may delegate to other senior officials within the entity concerned specific obligation under this Regulation. Regardless of possible delegation of its specific obligation, the highest level of management shall/may/can be held liable for the non-compliance by the entities with the obligations under this Regulation.</u></i></p> <p>put to political level</p> <p>Text Origin: Council Mandate</p>
Article 4(3b)			
66b			<p>3b. The highest level of management of each Union entity shall ensure that the Union entities approve the cybersecurity plan that includes cybersecurity risk management measures, in accordance with their risk analysis, so that the</p> <p><i><u>3b. The highest level of management of each Union entity shall approve the cybersecurity plan that includes cybersecurity risk management measures, in accordance with their risk analysis, so that the</u></i></p>

			framework is implemented in accordance with this Regulation.	<p>this Regulation.</p> <p>links to 75 Council to check</p> <p>Text Origin: Council Mandate</p>
Article 4(4)				
67	4. Each Union institution, body and agency shall have effective mechanisms in place to ensure that an adequate percentage of the IT budget is spent on cybersecurity.	4. Each Union institution, body and agency entity shall have effective mechanisms in place to ensure that an adequate percentage of the IT ICT budget is spent on cybersecurity.	deleted	<p>4. Each Union institution, body and agency entity shall have effective mechanisms in place to ensure that an adequate percentage of the IT ICT budget is spent on cybersecurity. Due account shall be taken of the framework when defining this percentage.</p> <p>Council to check about ICT</p> <p>Text Origin: EP Mandate</p>
Article 4(5)				
68	5. Each Union institution, body and agency shall appoint a Local Cybersecurity Officer or an equivalent function who shall act as its single point of contact regarding all aspects of cybersecurity.	5. Each Union institution, body and agency entity shall appoint a Local Cybersecurity Officer or an equivalent function who shall act as its single point of contact regarding all aspects of cybersecurity. Local Cybersecurity Officers may be shared by several Union entities.	5. Each Union institution, body and agency entity shall appoint a Local Cybersecurity Officer or an equivalent function who shall act as its single point of contact regarding all aspects of cybersecurity. The Local Cybersecurity Officer shall facilitate the	<p>5. Each Union institution, body and agency entity shall appoint a Local Cybersecurity Officer or an equivalent function who shall act as its single point of contact regarding all aspects of cybersecurity. The Local Cybersecurity Officer shall facilitate the implementation</p>

implementation of this Regulation and directly report to the highest level of management on a regular basis on the state of the implementation. Without prejudice to the Local Cybersecurity Officer being a single point of contact in each Union entity, a Union entity may delegate certain tasks of Local Cybersecurity Officer with respect to the implementation of this Regulation to CERT-EU on the basis of a service level agreement concluded between that Union entity and CERT-EU. The IICB shall decide whether the provision of this service shall be part of the baseline services of CERT-EU, taking into account the human and financial resources of the concerned Union entity. Appointed Local Cybersecurity Officers and any subsequent change thereto shall be notified by each Union entity to CERT-EU without undue delay. CERT-EU shall keep the regularly updated list of appointed Local Cybersecurity Officers.

of this Regulation and directly report to the highest level of management on a regular basis on the state of the implementation. Without prejudice to the Local Cybersecurity Officer being a single point of contact in each Union entity, a Union entity may delegate certain tasks of Local Cybersecurity Officer with respect to the implementation of this Regulation to CERT-EU on the basis of a service level agreement concluded between that Union entity and CERT-EU, or these tasks may be shared by several Union entities. In case these tasks are delegated to CERT-EU, the IICB shall decide whether the provision of this service shall be part of the baseline services of CERT-EU, taking into account the human and financial resources of the concerned Union entity. Appointed Local Cybersecurity Officers and any subsequent change thereto shall be notified by each Union entity to CERT-EU without undue delay. CERT-EU shall keep the regularly updated list of appointed Local Cybersecurity Officers.

Text Origin: Council Mandate

Article 4(6)				
68a			<p>6. The senior officials within the meaning of Article 29(2) of the Staff Regulations⁵ or other officials at equivalent level, of each Union entity shall follow specific trainings on a regular basis to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risk and management practices and their impact on the operations of the organisation.</p> <p>5. Regulation No 259/68 of the Council of 29 February 1968 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities, OJ L 56 of 4 March 1968.</p>	<p><u>6. The senior officials within the meaning of Article 29(2) of the Staff Regulations⁵ or other officials at equivalent level, of each Union entity, as well as all relevant staff tasked with implementing the cybersecurity risk-management measures and obligations laid down in this Regulation shall follow specific trainings on a regular basis to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risk and management practices and their impact on the operations of the organisation.</u></p> <p><u>5. Regulation No 259/68 of the Council of 29 February 1968 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities, OJ L 56 of 4 March 1968.</u></p> <p>EP text moved from row 71</p> <p>Text Origin: Council Mandate</p>
Article 4(7)				
68b			7. Each Union entity shall have effective mechanisms in place to	

			ensure that an adequate percentage of the IT budget is spent on cybersecurity. Due account shall be taken of the framework when defining this percentage.	
Article 5				
69	Article 5 Cybersecurity baseline	Article 5 Cybersecurity baseline risk-management measures	Article 5 Cybersecurity baseline risk management measures	Article 5 Cybersecurity baseline risk management measures Text Origin: Council Mandate
Article 5(1)				
70	1. The highest level of management of each Union institution, body and agency shall approve the entity's own cybersecurity baseline to address the risks identified under the framework referred to in Article 4(1). It shall do so in support of its mission and exercising its institutional autonomy. The cybersecurity baseline shall be in place by at the latest [18 months after the entry into force of this Regulation] and shall address the domains listed in Annex I and the measures listed in Annex II.	1. The highest level of management of each Union institution, body and agency entity shall approve the Union entity's own cybersecurity baseline risk-management measures to address the risks identified under the framework referred to in Article 4(1). It shall do so in support of its mission and exercising its institutional autonomy. The , in line with any guidance and recommendations of IICB and CERT-EU. Taking into account the state-of-the-art and, where applicable, relevant European and international standards, or	1. Each Union entity shall, under the oversight of its The highest level of management ensure that appropriate and proportionate technical, operational and organisational measures to manage of each Union institution, body and agency shall approve the entity's own cybersecurity baseline to address the risks identified under the framework referred to in Article 4(1), and to prevent and/or minimise the impact of incidents, are taken. Having regard to the state of the art and, where applicable, relevant European	LS to check

		<p>available European cybersecurity baseline shall be in place by at the latest [18 months after the entry into force of this Regulation] and shall address the domains listed in Annex I and the certificates as defined in Article 2, point (11), of Regulation (EU) 2019/881, those risk-management measures shall ensure a level of security of network and information systems across the entirety of the ICT environment commensurate to the risks identified under the framework referred to in Article 4(1). When assessing the proportionality of those measures, due account shall be taken of the degree of the Union entity's exposure to risks, its size, the likelihood of occurrence of incidents and their severity, including their societal, economic and interinstitutional impact listed in Annex II.</p>	<p>and international standards, as well as the cost of implementation, those measures. It shall do so in support of its mission and exercising its institutional autonomy. The cybersecurity baseline shall be in place by at the latest [18 months after the entry into force of this Regulation] and ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall address the domains listed in Annex I and the measures listed in Annex II be taken of the degree of the entity's exposure to risks, its size, the likelihood of occurrence of incidents and their severity, including their societal and economic impact.</p>	
Article 5(1a)				
70a		<p>1a. Union entities shall include at least the following domains in the implementation of the cybersecurity risk-management measures:</p>	<p>3. Union entities shall address at least the following specific domains in the implementation of the cybersecurity risk management measures within their cybersecurity plans, in line</p>	<p>Linked to row 70</p>

			with the guidance documents and recommendations from the IICB:	
Article 5(1a), point (a)				
70b		(a) cybersecurity policy, including measures needed to reach objectives and priorities referred to in Article 4 and paragraph 2a of this Article;	3a. cybersecurity policy, in terms of specification of the tools and measures needed to reach the objectives and priorities referred to in Article 4 and in Article 5(4);	<p><u>(a) cybersecurity policy, including measures needed to reach objectives and priorities referred to in Article 4 and paragraph 2a of this Article;</u></p> <p>Text Origin: EP Mandate</p>
Article 5(1a), point (b)				
70c			3b risk analysis and information system security policies;	<p><u>3b risk analysis and information system security policies;</u></p> <p>Text Origin: Council Mandate</p>
Article 5(1a), point (c)				
70d		(b) policy objectives regarding the use of cloud computing services as defined in Article 6, point (30), of Directive (EU) 2022/2555 and technical arrangements to enable and sustain teleworking;		<p><u>(b) policy objectives regarding the use of cloud computing services as defined in Article 6, point (30), of Directive (EU) 2022/2555 ;</u></p> <p>second part of the EP text moved to row 71b</p> <p>Text Origin: EP Mandate</p>

Article 5(1a), point (d)

70e		<p>(c) in order to assess whether Union entities have sufficient control over the security of their ICT systems, a complete cybersecurity initial review, including a risk, vulnerability and threat assessment, and a penetration-test of the ICT systems and devices of the Union entities to be carried out by a leading and verified third party external to the Union entities, such as a leading cybersecurity company, on ... [the date of entry into force of this Regulation] and every following year thereafter, which takes due account of the information security requirements of the relevant institutions;</p>	<p>PUBLIC</p>	<p><u>(d) COM proposal:</u> <u>the modalities of conducting regular cybersecurity reviews including risk, vulnerability and threat assessment in order to assess the level of control over the security of their ICT systems</u></p> <p>EP to propose compromise text</p>
-----	--	--	---------------	---

Article 5(1a), point (e)

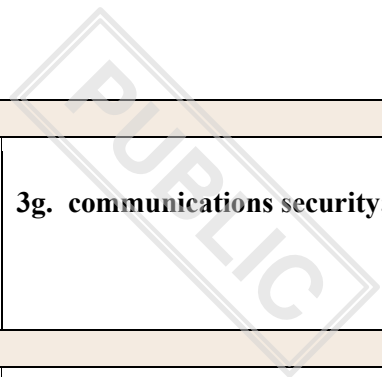
70f		<p>(e) in light of the reviews referred to in point (c), mitigation of the reported risks and vulnerabilities in cybersecurity updates, and implementation of the recommendations by means of cybersecurity policy which may include the replacement of</p>		<p>linked to row 70e</p>
-----	--	---	--	--------------------------

		infected ICT systems;		
Article 5(1a), point (f)				
70g		(f) organisation of cybersecurity, including definition of roles and responsibilities;	3c. organisation of cybersecurity, including definition of roles and responsibilities;	<u>(f) organisation of cybersecurity, including definition of roles and responsibilities;</u> Text Origin: EP Mandate
Article 5(1a), point (g)				
70h		(g) management of ICT environment, including ICT asset inventory and ICT network cartography;	3d. asset management, including IT asset inventory and IT network cartography;	<u>3d. asset management, including [ICT] asset inventory and [ICT] network cartography;</u> linked to inclusion of a definition of ICT environment Text Origin: Council Mandate
Article 5(1a), point (h)				
70i		(h) access control, identity management and privileged access management;	3e. human resources security and access control;	<u>3e. human resources security and access control;</u> Text Origin: Council Mandate
Article 5(1a), point (i)				
70j		(i) operations security and human resources security;	3f. operations security;	<u>3f. operations security;</u>

PUBLIC

human resources security moved to row 70i

Text Origin: Council Mandate



Article 5(1a), point (j)					
G	70k	(j) communications security;	3g. communications security;	<u>3g. communications security;</u> Text Origin: Council Mandate	G
Article 5(1a), point (k)					
Y	70l	(k) system acquisition, development, maintenance and transparency of the source code;	3h. system acquisition, development and maintenance, including vulnerability handling and disclosure;	EP to check	Y
Article 5(1a), point (l)					
Y	70m	(l) cybersecurity audits;		overall discussion on audits	Y
Article 5(1a), point (m)					
Y	70n	(m) ICT staff workload and overall satisfaction;		COM to propose a recital instead	Y
Article 5(1a), point (n)					
G	70o	(n) supply chain security and supplier relationships between Union entities and their direct suppliers and service providers;	3i supply chain security including security related aspects concerning the relationships between each Union entity and	<u>3i supply chain security including security related aspects concerning the relationships between each Union entity and its</u>	G

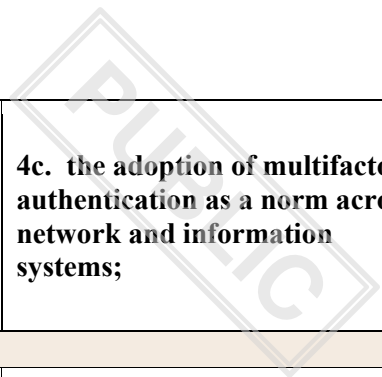
			its direct suppliers or service provider. Union entities shall take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures;	<u>direct suppliers or service provider. Union entities shall take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures;</u> Text Origin: Council Mandate
Article 5(1a), point (o)				
70p		(o) incident handling, including approaches to improve the preparedness, detection, analysis, and containment of, response to and recovery from incidents and cooperation with CERT-EU, such as the maintenance of security monitoring and logging;	3j. incident handling and cooperation with CERT-EU, such as the maintenance of security monitoring and logging;	<u>3j. incident handling and cooperation with CERT-EU, such as the maintenance of security monitoring and logging;</u> Text Origin: Council Mandate
Article 5(1a), point (p)				
70q		(p) business continuity management and crisis management; and	3k. business continuity management, such as back-up management and disaster recovery, and crisis management; and	<u>3k. business continuity management, such as back-up management and disaster recovery, and crisis management; and</u> Text Origin: Council Mandate

Article 5(1a), point (q)				
70r		(q) skills, education, awareness-raising, training programmes and exercises.	3l. promoting and developing cybersecurity education, skills, awareness-raising, exercise and training programmes.	<u>3l. promoting and developing cybersecurity education, skills, awareness-raising, exercise and training programmes.</u> Text Origin: Council Mandate
Article 5(2)				
71	2. The senior management of each Union institution, body and agency shall follow specific trainings on a regular basis to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risk and management practices and their impact on the operations of the organisation.	2. The senior management of each Union institution, body and agency entity, as well as all relevant staff tasked with implementing the cybersecurity risk-management measures and obligations laid down in this Regulation, shall follow specific trainings on a regular basis to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risk and management practices and their impact on the operations of the organisation Union entity.	2. The senior management of each Union institution, body and agency shall follow specific trainings on a regular basis to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risk and management practices and their impact on the operations of the organisation.	2. The senior management of each Union institution, body and agency shall follow specific trainings on a regular basis to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risk and management practices and their impact on the operations of the organisation. <u>deleted</u> EP text moved to row 68a
Article 5(2a)				
71a		2a. Union entities shall address at least the following specific	4. Union entities shall address at least the following specific	EP to check

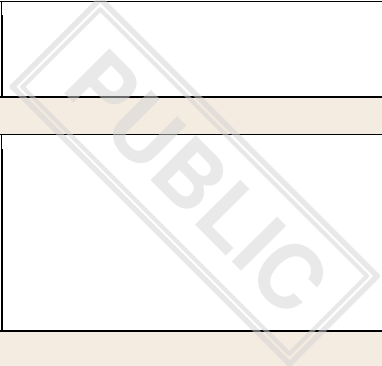
		measures and sub-controls in the implementation of the cybersecurity risk-management measures in their cybersecurity plans, in line with the guidance documents and recommendations of the IICB:	cybersecurity risk management measures in the implementation of the cybersecurity risk management measures within their cybersecurity plans, in line with the guidance documents and recommendations from the IICB:	
Article 5(2b)				
g	71b		4a. objectives and priorities regarding the use of cloud computing services within the meaning of Article 4(19) of Directive [proposal NIS 2] and technical arrangements to enable teleworking;	<p><u>4a. technical arrangements to enable and sustain teleworking;</u></p> <p>first part of the Council mandate moved to row 70d</p> <p>Text Origin: Council Mandate</p>
Article 5(2c)				
y	71c	(a) concrete steps for moving towards Zero Trust Architecture within the meaning of a security model comprised of a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries;	4b. concrete steps for future use of Zero Trust principles, including a security model, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries;	Council to check



PUBLIC



G	71d	(b) the adoption of multifactor authentication as a norm across network and information systems;	4c. the adoption of multifactor authentication as a norm across network and information systems;	G
Article 5(2d)				
Y	71e	(c) the use of cryptography and encryption, and in particular end-to-end encryption, encryption in transit, and encryption at rest as well as secure digital signing;	4f the use of cryptography and encryption, and in particular end-to-end encryption;	Council to check Y
Article 5(2e)				
Y	71f	(d) secured voice, video and text communications, and secured emergency communications systems, where appropriate;		Council to check; linked with row 71p Y
Article 5(2f)				
Y	71g	(e) the establishment of frequent and ad-hoc scanning capabilities of endpoint devices and other components of the ICT environment to detect and remove malware software such		Council to check Y

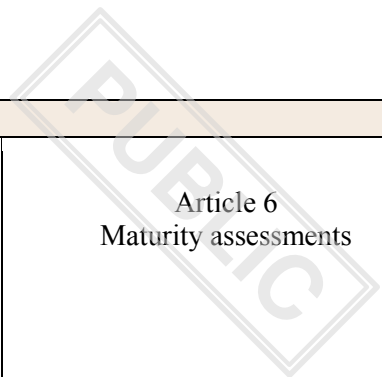


		as spyware;			
Article 5(2g)					
Y	71h	(f) ensuring privacy by design and the enhanced security of all personal data;		EP to check whether a recital instead	Y
Article 5(2g), point (a)					
G	71i	(g) the establishment of software supply chain security through criteria for secure software development and evaluation;	4d. the establishment of software supply chain security through criteria for secure software development and evaluation;	<u>4d. the establishment of software supply chain security through criteria for secure software development and evaluation;</u> Text Origin: Council Mandate	G
Article 5(2g), point (b)					
Y	71j	(h) regular cybersecurity training of staff members;		EP to propose a compromise, linked to row 71o	Y
Article 5(2g), point (c)					
Y	71k	(i) participation in interconnectivity risk analyses between the Union entities;		EP to check	Y

Article 5(2g), point (d)				
G	71l	(j) the enhancement of procurement rules to facilitate a high common level of cybersecurity through:	4e. the enhancement of procurement rules to facilitate a high common level of cybersecurity through:	<p><u>4e. the enhancement of procurement rules to facilitate a high common level of cybersecurity through:</u></p> <p>Text Origin: Council Mandate</p>
Article 5(2g), point (d)(i)				
Y	71m	(i) the removal of contractual barriers that limit information sharing from ICT service providers about incidents, vulnerabilities and cyber threats with CERT-EU;	4e(i) the removal of contractual barriers that limit information sharing from IT service providers about incidents, vulnerabilities and cyber threats with CERT-EU;	<p><u>(i) the removal of contractual barriers that limit information sharing from [ICT] service providers about incidents, vulnerabilities and cyber threats with CERT-EU;</u></p> <p>linked to definition of ICT environment</p> <p>Text Origin: EP Mandate</p>
Article 5(2g), point (d)(ii)				
Y	71n	(ii) the contractual obligation to report incidents, vulnerabilities, near misses and cyber threats as well as to have appropriate incidents response and monitoring in place;	4e(ii) the contractual obligation to report incidents, vulnerabilities and cyber threats as well as to have appropriate incidents response and monitoring in place;	<p>Council to check the addition of "near misses"</p>

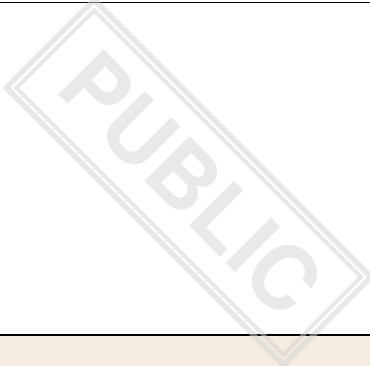


Article 5(2g), point (d)(iii)				
71o		(k) the establishment and adoption of training programmes on cybersecurity commensurate to the prescribed tasks and expected capabilities for the highest level of management and technical and operational staff.		EP to propose a compromise, linked to row 71j
Article 4				
71p			4g. secured communication systems within the organisation.	2h. Council to check, linked to row 71f
Article 5(2i)				
71q		2c. The IICB may recommend technical and methodological requirements of the domains and cybersecurity risk-management measures referred to in paragraphs 1a and 2a of this Article and, where necessary, recommend adaptations to reflect developments in cyberattack methods, cyber threats and technological progress, for the purpose of the review referred to in Article 24.		EP and Council to check



Article 6					
G	72	Article 6 Maturity assessments	Article 6 Cybersecurity maturity assessments	Article 6 Maturity assessments	Article 6 Cybersecurity maturity assessments Text Origin: EP Mandate
Article 6(1)					
Y	73	Each Union institution, body and agency shall carry out a cybersecurity maturity assessment at least every three years, incorporating all the elements of their IT environment as described in Article 4, taking account of the relevant guidance documents and recommendations adopted in accordance with Article 13.	1. Each Union institution, body and agency shall carry out a cybersecurity maturity assessment by ... [18 months after the date of entry into force of this Regulation], and at least every threetwo years thereafter, incorporating all the elements of their IT ICT environment as described in Article 4, taking account of the relevant guidance documents and recommendations adopted in accordance with Article 13.	1. Each Union entity shall, where appropriate with the assistance of a specialised third-party, institution, body and agency shall carry out a cybersecurity maturity assessment at least every three years, incorporating all the elements of their IT environment as described in Article 4, taking account of the relevant guidance documents and recommendations adopted in accordance with Article 13.	EP to check; COM to present an overview of timelines
Article 6, first paragraph a					
Y	73a			2. The IICB, upon the recommendation of CERT-EU and after consulting the European Union Agency for	Linked to row 73d

			Cybersecurity (ENISA), shall adopt, within 4 months of this Regulation entering into force, methodological guidelines on conducting maturity assessments.	
Article 6, first paragraph b				
Y	73b		2. Small Union entities with similar tasks or structure may carry out a combined cybersecurity maturity assessment.	Council to check
Article 6, first paragraph c				
Y	73c		3. Upon completion of the maturity assessment, the Union entity shall submit it to the IICB. The first maturity assessment shall be carried out [12 months after the entry into force of this Regulation] at the latest.	Linked to rows 73, 73e and 79
Article 6, first paragraph d				
Y	73d		3. The IICB, after consulting the European Union Agency for Cybersecurity (ENISA) and upon receiving guidance from CERT-EU, shall by ... [one year	Linked to row 73a



		after the date of entry into force of this Regulation], issue guidelines to Union entities for the purpose of carrying out cybersecurity maturity assessments. The cybersecurity maturity assessment shall be based on cybersecurity audits.		
Article 6, first paragraph e				
73e		<i>4. Upon request of the IICB, and with the explicit consent of the Union entity concerned, the results of a cybersecurity maturity assessment may be discussed within the IICB or within the established network of Local Cybersecurity Officers with a view to learning from experiences in the implementation of this Regulation and sharing best practices and results of use cases.</i>		<p>Linked to row 73 c , 79 and 120c</p> <p>Council to check</p>
Article 7				
74	Article 7 Cybersecurity plans	Article 7 Cybersecurity plans	Article 7 Cybersecurity plans	<p>Article 7 Cybersecurity plans</p> <p>Text Origin: Commission Proposal</p>

Article 7(1)

75	<p>1. Following the conclusions derived from the maturity assessment and considering the assets and risks identified pursuant to Article 4, the highest level of management of each Union institution, body and agency shall approve a cybersecurity plan without undue delay after the establishment of the risk management, governance and control framework and the cybersecurity baseline. The plan shall aim at increasing the overall cybersecurity of the concerned entity and shall thereby contribute to the achievement or enhancement of a high common level of cybersecurity among all Union institutions, bodies and agencies. To support the entity's mission on the basis of its institutional autonomy, the plan shall at least include the domains listed in Annex I, the measures listed in Annex II, as well as measures related to incident preparedness, response and recovery, such as security monitoring and logging. The plan shall be revised at least</p>	<p>1. Following the conclusions derived from the cybersecurity maturity assessment and considering the assets and risks identified pursuant to Article 4, the highest level of management of each Union institution, body and agencyentity shall approve a cybersecurity plan without undue delay after the establishment of the risk management, governance and control framework and the cybersecurity baseline. The risk-management measures. The cybersecurity plan shall aim at increasing the overall cybersecurity of the concernedUnion entity concerned and shall thereby contribute to the achievement or enhancement of a high common level of cybersecurity among all within the Union institutions, bodies and agencies. To support the Union entity's mission on the basis of its institutional autonomy, the cybersecurity plan shall at least include the domains listed in Annex I, the measures listed in Annex II, as well as measures related to incident preparedness,</p>	<p>1. Following the conclusions derived from the maturity assessment and considering the assets and risks identified pursuant to Article 4, the highest level of management of each Union institution, body and agency entity shall approve a cybersecurity plan without undue delay after the establishment of the I framework, adoption of the cybersecurity risk management, governance and control framework and the cybersecurity baseline. The measures and carrying out of the maturity assessment and no later than 21 months after the entry into force of this Regulation. The cybersecurity plan shall aim at increasing the overall cybersecurity of the concerned Union entity concerned and shall thereby contribute to the achievement or enhancement of a high common level of cybersecurity among all Union institutions, bodies and agenciesentities. To support the entity's mission on the basis of its institutional autonomy, the The cybersecurity plan shall at least</p>	<p>To be discussed with overall timeline</p>
----	--	--	--	--

	every three years, following the maturity assessments carried out pursuant to Article 6.	response and recovery, such as security monitoring and logging. The plan shall be revised at least every three years cybersecurity risk-management measures referred to in Article 5(1a) and (2a). The cybersecurity plan shall be revised at least every two years, or where necessary, with any substantial revision of the framework referred to in Article 4, following the cybersecurity maturity assessments carried out pursuant to Article 6.	include the domains listed in Annex I, the cybersecurity risk management measures listed in Annex II, as well as measures related to incident preparedness, response and recovery, such as security monitoring and logging <p>pursuant to Article 5 . The cybersecurity plan shall be revised at least every three-two years, following theor following each maturity assessmentsassessment carried out pursuant to Article 6 or every review of the framework pursuant to Article 4.</p>	
Article 7(2)				
76	2. The cybersecurity plan shall include staff members' roles and responsibilities for its implementation.	2. The cybersecurity plan shall include relevant staff members' roles, required level of competence and responsibilities for its implementation, including detailed job descriptions for technical and operational staff as well as all relevant processes underpinning performance evaluation.	<i>deleted</i>	<i>COM to propose a compromise</i>
Article 7(2a)				
76a		2a. The cybersecurity plan shall include the Union entity's cyber		<i>Linked to row 120h;</i>

		crisis management plan for major incidents.		to be discussed together with Art.22	
Article 7(3)					
Y	77	3. The cybersecurity plan shall consider any applicable guidance documents and recommendations issued by CERT-EU.	3. The cybersecurity plan shall consider any applicable guidance documents and recommendations issued by CERT-EU in accordance with Article 13 or any applicable or targeted recommendations issued by the IICB and CERT-EU.	3. The cybersecurity plan shall consider take into account any applicable guidance documents and recommendations issued by CERT-EU in accordance with Article 13 .	Council to propose compromise based on EP text Linked to rows 119a, 119b and 120f
Article 7(4)					
G	77a		3a. The Union entities shall submit their cybersecurity plans to the IICB.	4. Upon completion of the cybersecurity plan, the Union entity shall submit it to the IICB.	<u>4. Upon completion of the cybersecurity plan, the Union entity shall submit it to the IICB.</u> Text Origin: Council Mandate
Article 7(a)					
Y	77b			Article 7a Peer Review	Linked to row 112c
Article 7(a) 1					
Y	77c			1. The IICB shall, upon the recommendation of CERT-EU and after consulting ENISA,	

establish, at the latest by ... [24 months following the entry into force of this Regulation], using the methodology for peer reviews and methodology for self-assessment in accordance with Article 16 of Directive [proposal NIS 2] adapted where necessary to the needs of the Union entities, the methodology and organisational aspects of a peer review with a view to learning from shared experiences, strengthening mutual trust, achieving a high common level of cybersecurity, as well as enhancing the Union entities cybersecurity capabilities and policies necessary to implement this Regulation. Participation in the peer reviews is voluntary. Representatives from Member States may participate in the peer review as observers. The peer reviews shall be conducted by cybersecurity experts assigned by at least two Union entities, different from the Union entities being reviewed and shall cover at least one of the following:

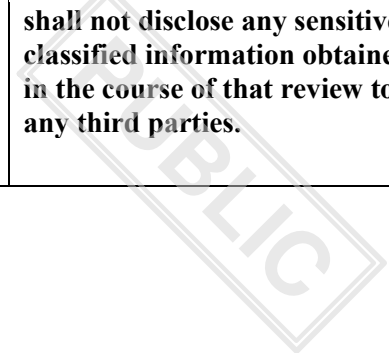
Article 7(a) 1 i

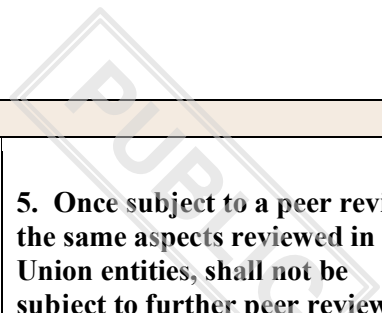
77d

			(i) the level of implementation of the cybersecurity risk management measures and reporting obligations referred to in Articles 5 and 20;	
Article 7(a) 1 ii				
Y	77e		(ii) the level of capabilities, including the available financial, technical and human resources;	Y
Article 7(a) 1 iii				
Y	77f		(iii) the level of implementation of the information-sharing framework, referred to in Article 19;	Y
Article 7(a) 1 iv				
Y	77g		(iv) specific issues of cross-sector nature.	Y
Article 7(a) 2				
Y	77h		2. Union entities may identify specific issues mentioned in paragraph 1, point (iv) to be reviewed. The scope of the	Y

			<p>review, including identified issues, shall be communicated to the participating Union entities prior to the commencement of the peer review.</p>	
Article 7(a) 3				
77i			<p>3. Prior to the commencement of the peer review, Union entities may carry out a self-assessment of the reviewed aspects and provide that self-assessment to the designated experts.</p>	
Article 7(a) 4				
77j			<p>4. Peer reviews shall entail physical or virtual on-site visits and off-site exchanges. In view of the principle of good cooperation, the Union entities subject to the peer review shall provide the designated experts with the information necessary for the assessment, without prejudice to national or Union laws concerning protection of sensitive or classified information. Any information obtained through the peer review process shall be used solely for that purpose. The experts participating in the peer review</p>	

			shall not disclose any sensitive or classified information obtained in the course of that review to any third parties.	
--	--	--	--	--



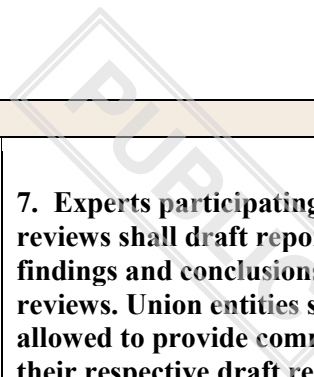


Article 7(a) 5

77k			<p>5. Once subject to a peer review, the same aspects reviewed in the Union entities, shall not be subject to further peer review in that Union entities for the two years following the conclusion of the peer review, unless otherwise requested by the Union entities or agreed upon after a proposal by the IICB.</p>	
-----	--	--	--	--

Article 7(a) 6

77l			<p>6. Union entities shall ensure that any risk of conflict of interests concerning the designated experts are revealed to the other Union entities and the IICB, before the commencement of the peer review. The Union entities subject to the peer review may object to the designation of particular experts on duly justified grounds communicated to the designating the Union entities.</p>	
-----	--	--	--	--

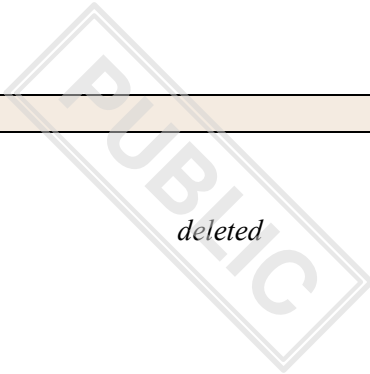


Article 7(a) 7

77m			<p>7. Experts participating in peer reviews shall draft reports on the findings and conclusions of the reviews. Union entities shall be allowed to provide comments on their respective draft reports, which shall be attached to the reports. The reports shall include recommendations to enable improvement on the aspects covered by the peer review. The reports shall be presented to the IICB and the CSIRTs network when relevant. Union entities under review may decide to make its report, or a redacted version of its report, publicly available.</p>	
-----	--	--	--	--

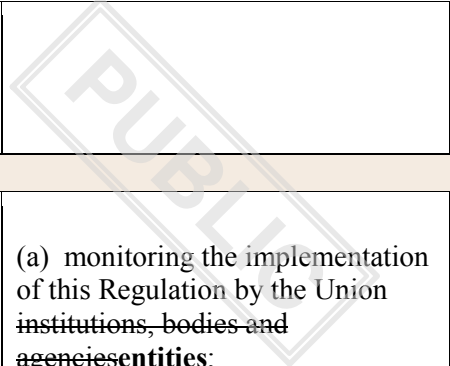
Article 8

78	Article 8 Implementation	Article 8 Implementation	Article 8 Implementation	Article 8 <i>Implementation</i> Article 8 deleted Text Origin: Commission Proposal
----	--------------------------	--------------------------	--------------------------	--



Article 8(1)				
79	<p>1. Upon completion of maturity assessments, the Union institutions, bodies and agencies shall submit these to the Interinstitutional Cybersecurity Board. Upon completion of security plans, the Union institutions, bodies and agencies shall notify the Interinstitutional Cybersecurity Board of the completion. Upon request of the Board, they shall report on specific aspects of this Chapter.</p>	<p>1. Upon completion of maturity assessments, the Union institutions, bodies and agencies shall submit these to the Interinstitutional their respective cybersecurity maturity assessments referred to in Article 6 and the cybersecurity Board. Upon completion of security plans plans referred to in Article 7, the Union institutions, bodies and agencies entities shall notify the Interinstitutional Cybersecurity Board of the completion submit them to the IICB. Upon request of the Board IICB, they shall report on specific aspects of this Chapter.</p>	<p><i>deleted</i></p>	<p>Moved to rows 73c, 122 +122b</p>
Article 8(2)				
80	<p>2. Guidance documents and recommendations, issued in accordance with Article 13, shall support the implementation of the provisions laid down in this Chapter.</p>	<p>2. Guidance documents and recommendations, issued in accordance with Article 13, shall support the implementation of the provisions laid down in this Chapter.</p>	<p>2. Guidance documents and recommendations, issued in accordance with Article 13, shall support the implementation of the provisions laid down in this Chapter.</p>	<p>2. Guidance documents and recommendations, issued in accordance with Article 13, shall support the implementation of the provisions laid down in this Chapter.</p> <p>Covered by Article 13 (row 147)</p>

				Text Origin: Commission Proposal
Article 8(3)				
80a			3. Upon request of the IICB, the Union entities shall report on specific aspects of this Chapter.	Covered by rows 122 + 122b
Chapter III				
81	Chapter III INTERINSTITUTIONAL CYBERSECURITY BOARD	Chapter III INTERINSTITUTIONAL CYBERSECURITY BOARD IICB	Chapter III INTERINSTITUTIONAL CYBERSECURITY BOARD	
Article 9				
82	Article 9 Interinstitutional Cybersecurity Board	Article 9 Interinstitutional Cybersecurity Board IICB	Article 9 Interinstitutional Cybersecurity Board	
Article 9(1)				
83	1. An Interinstitutional Cybersecurity Board (IICB) is established.	1. An Interinstitutional Cybersecurity Board (IICB) IICB is established.	1. An Interinstitutional Cybersecurity Board (IICB) is established.	
Article 9(2)				
84	2. The IICB shall be responsible for:	2. The IICB shall be responsible for:	2. The IICB shall be responsible for:	2. The IICB shall be responsible for:



				Text Origin: Commission Proposal
Article 9(2), point (a)				
85	(a) monitoring the implementation of this Regulation by the Union institutions, bodies and agencies;	(a) monitoring the implementation of this Regulation by the Union institutions, bodies and agencies entities and providing recommendations for achieving a high common level of cybersecurity;	(a) monitoring the implementation of this Regulation by the Union institutions, bodies and agencies entities;	
Article 9(2), point (b)				
86	(b) supervising the implementation of general priorities and objectives by CERT-EU and providing strategic direction to CERT-EU.	(b) supervising the implementation of general priorities and objectives by CERT-EU and providing strategic direction to CERT-EU.	(b) supervising the implementation of general priorities and objectives by CERT-EU and providing strategic direction to CERT-EU.	(b) supervising the implementation of general priorities and objectives by CERT-EU and providing strategic direction to CERT-EU. Text Origin: Commission Proposal
Article 9(3)				
86a		3. The IICB shall consist of	3. The IICB shall consist of:	
Article 9(3), point (a)				
86b		(a) two representatives designated by each of the	a) one representative designated by each of the following:	

		following:		
Article 9(3), point (a) i				
86c		(i) the European Parliament;	(i) the European Parliament;	
Article 9(3), point (a) ii				
86d		(ii) the Council of the European Union;	(ii) the European Council	
Article 9(3), point (a) iii				
86e		(iii) the European Commission;	(iv) the European Commission;	
86f		(b) one representative designated by each of the following:		
Article 9(3), point (a) iv				
86g			(iii) the Council of the European Union;	
Article 9(3), point (a) v				
86h		(i) the Court of Justice of the European Union;	(v) the Court of Justice of the European Union;	

--	--	--	--	--

PUBLIC

Article 9(3), point (a) vi				
86i		(ii) the European Central Bank;	(vi) the European Central Bank;	
Article 9(3), point (a) vii				
86j		(iii) the European Court of Auditors;	(vii) the European Court of Auditors;	
Article 9(3), point (a) viii				
86k		(iv) the European External Action Service;	(viii) the European External Action Service;	
Article 9(3), point (a) ix				
86l		(v) the European Economic and Social Committee;	(ix) the European Economic and Social Committee;	
Article 9(3), point (a) x				
86m		(vi) the European Committee of the Regions;	(x) the European Committee of the Regions;	
Article 9(3), point (a) xi				
86n		(vii) the European Investment Bank;	(xi) the European Investment Bank;	

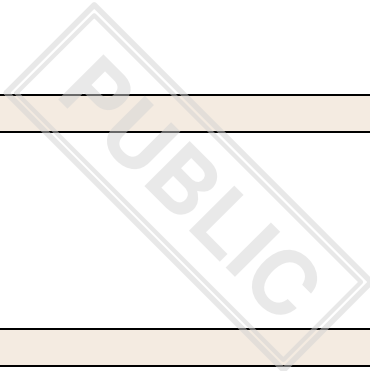
Article 9(3), point (a) xii				
86o		(x) the European Cybersecurity Industrial, Technology and Research Competence Centre;	(xii) the European Cybersecurity Industrial, Technology and Research Competence Centre; and	
Article 9(3), point (a) xiii				
86p		(viii) ENISA;	(xiii) the European Union Agency for Cybersecurity;	
86q		(ix) the European Data Protection Supervisor (EDPS);		
86r		(xi) the European Union Agency for the Space Programme;		
Article 9(3), first subparagraph				
87	3. The IICB shall consist of three representatives nominated by the Union Agencies Network (EUAN) upon a proposal of its ICT Advisory Committee to represent the interests of the agencies and bodies that run their own IT	3-(c) The IICB shall consist of three representatives nominated representative designated by the Union Agencies Network (EUAN) upon a proposal of its ICT Advisory Committee to represent the interests of the agencies, offices	33b. The ICB shall consist of three representatives nominated designated by the Union Agencies Network (EUAN) upon a proposal of its ICT Advisory Committee to represent the interests of the agencies and bodies that run their	

	environment and one representative designated by each of the following:	and bodies that run their own IT environment and one representative designated by each of the following: other than those referred to in points (b)(viii), (x) and (xi) and that runs its own ICT environment.	own IT environment and one representative designated by each of the following:	
<i>Article 9(3), first subparagraph, point (a)</i>				
88	(a) the European Parliament;	<i>deleted</i>	<i>deleted</i>	
<i>Article 9(3), first subparagraph, point (b)</i>				
89	(b) the Council of the European Union;	<i>deleted</i>	<i>deleted</i>	
<i>Article 9(3), first subparagraph, point (c)</i>				
90	(c) the European Commission;	<i>deleted</i>	<i>deleted</i>	
<i>Article 9(3), first subparagraph, point (b)(ii)</i>				
91	(d) the Court of Justice of the European Union;	<i>deleted</i>	<i>deleted</i>	
<i>Article 9(3), first subparagraph, point (e)</i>				
92				

	(e) the European Central Bank;	<i>deleted</i>	<i>deleted</i>	
<i>Article 9(3), first subparagraph, point (f)</i>				
93	(f) the European Court of Auditors;	<i>deleted</i>	<i>deleted</i>	
<i>Article 9(3), first subparagraph, point (g)</i>				
94	(g) the European External Action Service;	<i>deleted</i>	<i>deleted</i>	
<i>Article 9(3), first subparagraph, point (h)</i>				
95	(h) the European Economic and Social Committee;	<i>deleted</i>	<i>deleted</i>	
<i>Article 9(3), first subparagraph, point (i)</i>				
96	(i) the European Committee of the Regions;	<i>deleted</i>	<i>deleted</i>	
<i>Article 9(3), first subparagraph, point (j)</i>				
97	(j) the European Investment Bank;	<i>deleted</i>	<i>deleted</i>	
<i>Article 9(3), first subparagraph, point (k)</i>				
98				

	(k) the European Union Agency for Cybersecurity.	<i>deleted</i>	<i>deleted</i>	
--	--	----------------	----------------	--

PUBLIC



<i>Article 9(3), second subparagraph</i>				
98a		Gender balance shall be aimed at among the appointed representatives.		
<i>Article 9(3a)</i>				
99	Members may be assisted by an alternate. Other representatives of the organisations listed above or of other Union institutions, bodies and agencies may be invited by the chair to attend IICB meetings without voting power.	3a. Members may be assisted by an alternate. Other representatives of the organisations listed above or of other Union institutions, bodies and agencies entities may be invited by the chair to attend IICB meetings without voting power.	3a. Members may be assisted by an alternate. Other representatives of the organisations entities listed above or of other Union institutions, bodies and agencies entities may be invited by the chair to attend IICB meetings without voting power.	
<i>Article 9(3b)</i>				
99a		3b. The head of CERT-EU and the chairs of the Cooperation Group, the CSIRTs network and the EU-CyCLONe, referred to in Articles 14, 15 and 16 of Directive (EU) 2022/2555, or their alternates, may participate in IICB meetings as observers. In exceptional cases, and in accordance with the internal rules of procedure of the IICB,		

		the IICB may decide otherwise.		
Article 9(4)				
100	4. The IICB shall adopt its internal rules of procedure.	4. The IICB shall adopt its internal rules of procedure.	4. The IICB shall adopt its internal rules of procedure.	4. The IICB shall adopt its internal rules of procedure. Text Origin: Commission Proposal
Article 9(5)				
101	5. The IICB shall designate a chair, in accordance with its internal rules of procedure, from among its members for a period of four years. His or her alternate shall become a full member of the IICB for the same duration.	5. The IICB shall designate a chair, in accordance with its internal rules of procedure, from among its members for a period of four years. His or her alternate shall become a full member with voting rights of the IICB for the same duration.	5. The IICB shall designate a chair, in accordance with its internal rules of procedure, from among its members for a period of four two years. His or her alternate shall become a full member of the IICB for the same duration.	
Article 9(6)				
102	6. The IICB shall meet at the initiative of its chair, at the request of CERT-EU or at the request of any of its members.	6. The IICB shall meet at the initiative of its chair, and at least two times a year , at the request of CERT-EU or at the request of any of its members.	6. The IICB shall meet at least three times a year at the initiative of its chair, and/or at the request of CERT-EU or and/or at the request of any of its members.	
Article 9(7)				
103	7. Each member of the IICB shall have one vote. The IICB's	7. Each member of the IICB shall have one vote. The IICB's	7. Each member of the IICB shall have one vote. The IICB's	7. Each member of the IICB shall have one vote. The IICB's

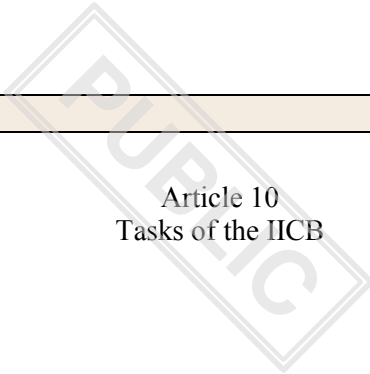
	decisions shall be taken by simple majority except where otherwise provided for in this Regulation. The chair shall not vote except in the event of a tied vote where he or she may cast a deciding vote.	decisions shall be taken by simple majority except where otherwise provided for in this Regulation. The chair shall not vote except in the event of a tied vote where he or she may cast a deciding vote.	decisions shall be taken by simple majority except where otherwise provided for in this Regulation. The chair shall not vote except in the event of a tied vote where he or she may cast a deciding vote.	decisions shall be taken by simple majority except where otherwise provided for in this Regulation. The chair shall not vote except in the event of a tied vote where he or she may cast a deciding vote. Text Origin: Commission Proposal
Article 9(8)				
104	8. The IICB may act by a simplified written procedure initiated in accordance with the internal rules of procedure of the IICB. Under that procedure, the relevant decision shall be deemed approved within the timeframe set by the chair, except where a member objects.	8. The IICB may act by a simplified written procedure initiated in accordance with the internal rules of procedure of the IICB. Under that procedure, the relevant decision shall be deemed approved within the timeframe set by the chair, except where a member objects.	8. The IICB may act by a simplified written procedure initiated in accordance with the internal rules of procedure of the IICB. Under that procedure, the relevant decision shall be deemed approved within the timeframe set by the chair, except where a member objects.	8. The IICB may act by a simplified written procedure initiated in accordance with the internal rules of procedure of the IICB. Under that procedure, the relevant decision shall be deemed approved within the timeframe set by the chair, except where a member objects. Text Origin: Commission Proposal
Article 9(9)				
105	9. The Head of CERT-EU, or his or her alternate, shall participate in IICB meetings except where otherwise decided by the IICB.	<i>deleted</i>	9. The Head of CERT-EU, or his or her alternate, shall the chair of the NIS Cooperation Group, the chair of EU-CyCLONe and the chair of the CSIRTs Network, or their alternates, may participate in	

			IICB meetings except where otherwise decided by the IICB, as observers .	
Article 9(10)				
106	10. The secretariat of the IICB shall be provided by the Commission.	10. The secretariat of the IICB shall be provided by the Commission.	10. The secretariat of the IICB shall be provided by ENISA and shall be accountable to the IICB chair the Commission.	
Article 9(11)				
107	11. The representatives nominated by the EUAN upon a proposal of the ICT Advisory Committee shall relay the IICB's decisions to the Union agencies and joint undertakings. Any Union agency and body shall be entitled to raise with the representatives or the chair of the IICB any matter which it considers should be brought to the IICB's attention.	11. The representatives representative nominated by the EUAN upon a proposal of the ICT Advisory Committee shall relay the IICB's decisions to the Union agencies and joint undertakings. Any Union agency and body shall be entitled to raise with the representatives or the chair of the IICB any matter which it considers should be brought to the IICB's attention.	11. The representatives nominated by the EUAN upon a proposal of the ICT Advisory Committee shall relay the IICB's decisions to the Union agencies and joint undertakings members of the EUAN . Any Union agency and body shall be entitled to raise with the representatives or the chair of the IICB any matter which it considers should be brought to the IICB's attention.	
Article 9(12)				
108	12. The IICB may act by a simplified written procedure initiated by the chair under which the relevant decision shall be	<i>deleted</i>	<i>deleted</i>	

	deemed approved within the timeframe set by the chair, except where a member objects.			
<i>Article 9(13)</i>				
109	13. The IICB may nominate an Executive Committee to assist it in its work, and delegate some of its tasks and powers to it. The IICB shall lay down the rules of procedure of the Executive Committee, including its tasks and powers, and the terms of office of its members.	13. The IICB may nominate an Executive Committee to assist it in its work, and delegate some of its tasks and powers to it. The IICB shall lay down the rules of procedure of the Executive Committee, including its tasks and powers, and the terms of office of its members.	13. The IICB may nominate establish an Executive Committee to assist it in its work, and delegate some of its tasks and powers to it, in particular those in Article 10 letters (c) and (e) . The IICB shall lay down the rules of procedure of the Executive Committee, including its tasks and powers, and the terms of office of its members.	
109a			14. The IICB shall submit a report to the Council every 12 months detailing the progress made with the implementation of this Regulation and specifying in particular the extent of cooperation of CERT-EU with its national counterparts in each of the Member States. This report shall constitute an input to the biennial Report on the state of cybersecurity in the Union over the same time period in accordance to Article 15 of Directive [proposal NIS 2].	

--	--	--	--	--

PUBLIC



Article 10				
110	Article 10 Tasks of the IICB	Article 10 Tasks of the IICB	Article 10 Tasks of the IICB	Article 10 Tasks of the IICB Text Origin: Commission Proposal
Article 10, first paragraph				
111	When exercising its responsibilities, the IICB shall in particular:	When exercising its responsibilities, the IICB shall in particular:	When exercising its responsibilities, the IICB shall in particular:	When exercising its responsibilities, the IICB shall in particular: Text Origin: Commission Proposal
111a		(-a) support Union entities in implementing this Regulation with the aim to raise their respective levels of cybersecurity;		
111b		(-aa) effectively monitor the implementation of the obligations of this Regulation in		

		Union entities without prejudice to their institutional autonomy and the overall institutional balance;		
111c		(-ab) provide strategic direction to the head of CERT-EU;		
Article 10, first paragraph, point (a)				
112	(a) review any reports requested from CERT-EU on the state of implementation of this Regulation by the Union institutions, bodies and agencies;	(a) review any request reports requested from CERT-EU on the state of implementation of this Regulation by the Union institutions, bodies and agencies entities;	(a) review any reports requested from CERT-EU on the state of implementation of this Regulation by the Union institutions, bodies and agencies effectively monitor and supervise the application of this Regulation and support the Union entities to strengthen their cybersecurity; to this end, the IICB may request ad-hoc reports from CERT-EU and Union entities;	
112a			(aa) following a strategic discussion, adopt a multiannual strategy on raising the level of cybersecurity in the Union entities and asses it on regular	

			basis and at least every five years and where necessary, amend it;	
112b		(aa) approve, on the basis of a proposal from the head of CERT-EU, recommendations for achieving a high common level of cybersecurity, addressed to one or more Union entities;		
112c		(ab) establish a framework for conducting of peer reviews for the Union entities with a view of learning from shared experiences, strengthening mutual trust, achieving a high common level of cybersecurity, as well as enhancing Union entities' capabilities, to be conducted by cybersecurity technical experts designated by an entity different from the entity being reviewed;		
Article 10, first paragraph, point (b)				
113	(b) approve, on the basis of a proposal from the Head of CERT-EU, the annual work programme	(b) approve, on the basis of a proposal from the Head of CERT-EU, the annual work programme	(b) approve, on the basis of a proposal from submitted by the Head of CERT-EU, the annual	

	for CERT-EU and monitor its implementation;	for CERT-EU and monitor its implementation;	work programme for CERT-EU and monitor its implementation;	
Article 10, first paragraph, point (c)				
114	(c) approve, on the basis of a proposal from the Head of CERT-EU, CERT-EU's service catalogue;	(c) approve, on the basis of a proposal from the Head of CERT-EU, CERT-EU's service catalogue;	(c) approve, on the basis of a proposal from the Head of CERT-EU, CERT-EU's service catalogue and any subsequent updates thereof;	
Article 10, first paragraph, point (d)				
115	(d) approve, on the basis of a proposal submitted by the Head of CERT-EU, the annual financial planning of revenue and expenditure, including staffing, for CERT-EU activities;	(d) approve, on the basis of a proposal submitted by the Head of CERT-EU, the annual financial planning of revenue and expenditure, including staffing, for CERT-EU activities;	(d) approve, on the basis of a proposal submitted by the Head of CERT-EU, the annual financial planning of revenue and expenditure, including staffing, for CERT-EU activities;	(d) approve, on the basis of a proposal submitted by the Head of CERT-EU, the annual financial planning of revenue and expenditure, including staffing, for CERT-EU activities; <small>Text Origin: Commission Proposal</small>
Article 10, first paragraph, point (e)				
116	(e) approve, on the basis of a proposal from the Head of CERT-EU, the modalities for service level agreements;	(e) approve, on the basis of a proposal from the Head of CERT-EU, the modalities for service level agreements;	(e) approve, on the basis of a proposal from the Head of CERT-EU, the modalities for service level agreements;	(e) approve, on the basis of a proposal from the Head of CERT-EU, the modalities for service level agreements; <small>Text Origin: Commission Proposal</small>

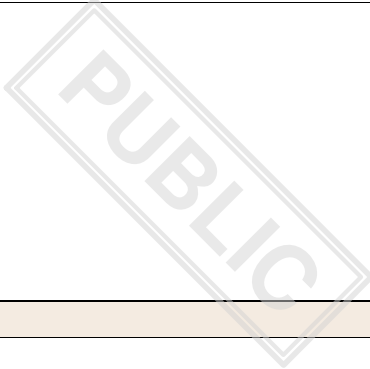
Article 10, first paragraph, point (f)				
117	(f) examine and approve the annual report drawn up by the Head of CERT-EU covering the activities of, and management of funds by CERT-EU;	(f) examine and approve the annual report drawn up by the Head of CERT-EU covering the activities of, and management of funds by CERT-EU;	(f) examine and approve the annual report drawn up by the Head of CERT-EU covering the activities of, and management of funds by CERT-EU;	(f) examine and approve the annual report drawn up by the Head of CERT-EU covering the activities of, and management of funds by CERT-EU; Text Origin: Commission Proposal
Article 10, first paragraph, point (g)				
118	(g) approve and monitor key performance indicators for CERT-EU defined on a proposal by the Head of CERT-EU;	(g) approve and monitor key performance indicators KPIs for CERT-EU defined on a proposal by the Head of CERT-EU;	(g) approve and monitor key performance indicators for CERT-EU defined on a proposal by the Head of CERT-EU;	
Article 10, first paragraph, point (h)				
119	(h) approve cooperation arrangements, service level arrangements or contracts between CERT-EU and other entities pursuant to Article 17;	(h) approve cooperation arrangements, service level arrangements or contracts between CERT-EU and other entities pursuant to Article 17;	(h) approve cooperation arrangements, service level arrangements agreements or contracts between CERT-EU and other entities pursuant to Article 17;	
119a		(ha) adopt guidance documents or recommendations on the basis of CERT-EU proposal;		

PUBLIC

119b		(hb) where necessary, instruct CERT-EU to issue, withdraw or modify a proposal for guidance documents or recommendations, or a call for action;	(j) adopt guidance documents and recommendations on the basis of a proposal from CERT-EU in accordance with Article 13 and instruct CERT-EU to issue, withdraw or modify a proposal for guidance documents or recommendations, or a call for action;	
Article 10, first paragraph, point (i)				
120	(i) establish as many technical advisory groups as necessary to assist the IICB's work, approve their terms of reference and designate their respective chairs.	(i) establish as many technical advisory groups as necessary with concrete tasks to assist the IICB's work, approve their terms of reference and designate their respective chairs-;	(i) establish as many technical advisory groups as necessary to assist the IICB's work, approve their terms of reference and designate their respective chairs-;	
120a		(ia) review and upon request, following relevant guidance from CERT-EU, provide feedback to Union entities' regarding the cybersecurity maturity assessments referred to in Article 6 and cybersecurity plans referred to in Article 7;		

Article 10, first paragraph, point (k)				
120b			(k) receive and assess documents and reports submitted by the Union entities under this Regulation;	
Article 10, first paragraph, point (k)				
120c		(ib) facilitate the exchange of best practices among the Local Cybersecurity Officers; provide, where appropriate, the recommendations on their role within the Union entities;	(l) support the establishment of an informal group gathering the Local Cybersecurity Officers of all the entities and thereby facilitate the exchange of best practices and information in relation to the implementation of this Regulation;	
Article 10, first paragraph, point (m)				
120d		(ic) review possible interconnections between Union entities' ICT environments and maintain an inventory of shared components of ICT products, ICT services and ICT processes;		
Article 10, first paragraph, point (m)				
120e			(m) develop a cyber crisis	

			<p>management plan to support the coordinated management of major incidents at operational level affecting Union entities and to contribute to the regular exchange of relevant information notably on impacts and severity of major incidents and the possible ways of mitigation.</p>	
120f		<p>(id) where appropriate, adopt recommendations on the interoperability of Union entities' ICT environments or components thereof;</p>		
120g		<p>(ie) support the establishment of a Cybersecurity Officers Group, to be coordinated by ENISA, comprising the Local Cybersecurity Officers of all Union entities with an aim to facilitate the sharing of best practices and experiences gained from the implementation of this Regulation;</p>		



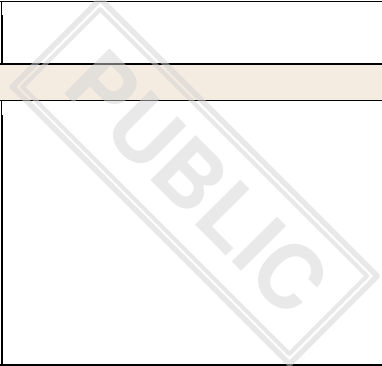
120h		(if) develop an incident and response plan for major incidents and coordinate the adoption of individual Union entities' cyber crisis management plans referred to in Article 7(2a);		
120i		(ig) adopt recommendations on the basis of the results of Union level coordinated security risk assessments of critical supply chains referred to in Article 22 of Directive (EU) 2022/2555 to support Union entities in adopting effective and proportionate cybersecurity risk-management measures relating to supply chain security referred to in Article 5(1a), point (m);		
120j		<i>(ih) develop guidelines for information sharing arrangements referred to in Article 19.</i>		
Article 11				
121				

	Article 11 Compliance	Article 11 Compliance	Article 11 Compliance	Article 11 Compliance Text Origin: Commission Proposal
Article 11, first paragraph				
122	<p>The IICB shall monitor the implementation of this Regulation and of adopted guidance documents, recommendations and calls for action by the Union institutions, bodies and agencies. Where the IICB finds that Union institutions, bodies or agencies have not effectively applied or implemented this Regulation or guidance documents, recommendations and calls for action issued under this Regulation, it may, without prejudice to the internal procedures of the relevant Union institution, body or agency:</p>	<p>1. The IICB shall monitor the implementation of this Regulation and of adopted guidance documents, recommendations and calls for action by the Union institutions, bodies and agencies. Where the IICB finds that Union institutions, bodies or agencies have not effectively applied or implemented this Regulation or guidance documents, recommendations and calls for action issued under this Regulation, it may, without prejudice to the internal procedures of the relevant Union institution, body or agency:entities.</p>	<p>1. The IICB shall, in accordance with Articles 9(2) and 10, effectively monitor the implementation of this Regulation and of adopted guidance documents, recommendations and calls for action by the Union institutions, bodies and agencies. Whereentities. To this end, the IICB finds that Union institutions, bodies or agencies have not effectively applied or implemented this Regulation or guidance documents, recommendations and calls for action issued under this Regulation, it may, without prejudice to the internal procedures of the relevant Union institution, body or agency:may request information or documentation necessary to assess the proper application of the provisions of the Regulation by the Union entities. For the purpose of adopting compliance measures under this Article the concerned Union entity shall not have</p>	

			voting rights.	
--	--	--	----------------	--

PUBLIC

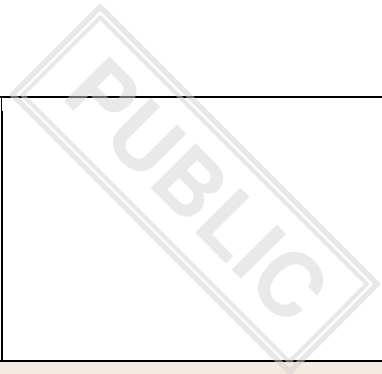
Article 11, second paragraph				
122a		<p>2. Where the IICB finds that Union entities have not effectively applied or implemented this Regulation or guidance documents, recommendations and calls for action issued under this Regulation, it may, without prejudice to the internal procedures of the relevant Union entity:</p>	<p>2. Where the IICB finds that Union entities have not effectively applied or implemented this Regulation or guidance documents, recommendations and calls for action issued under this Regulation, it may, without prejudice to the internal procedures of the relevant Union entity, and after having given the opportunity to the entity or the person concerned to present their views:</p>	
122b		<p>(-b) request relevant and available documentation of the Union entity concerned;</p>		
122c		<p>(-aa) communicate a reasoned opinion to the Union entity concerned with observed gaps in the implementation of this Regulation;</p>		



122d		(-ab) invite the Union entity concerned to provide a self-assessment on its reasoned opinion within a specified timeframe;		
122e		(-ac) provide, after consulting CERT-EU, guidance to the individual Union entity to bring its respective framework, cybersecurity risk-management measures, cybersecurity plans and reporting obligations in compliance with this Regulation within a specified period;		
Article 11, first paragraph, point (a)				
123	(a) issue a warning; where necessary in view of a compelling cybersecurity risk, the audience of the warning shall be restricted appropriately;	(a) issue a warning; where necessary in view of a compelling cybersecurity risk, the audience of the warning shall be restricted appropriately;	(a) issue a warning to address identified shortcomings within a specified timeframe, including recommendations to amend cybersecurity documents adopted by the Union entities based on this Regulation; where necessary in view of a compelling cybersecurity risk, the audience of	

			the warning shall be restricted appropriately;	
Article 11, first paragraph, point (b)				
123a			(aa) issue a reasoned notification to a Union entity, in case that shortcomings identified in the previously issued warning were not sufficiently addressed in a specified timeframe, and formally notify that opinion to the Council, the European Parliament and the Commission;	
Article 11, first paragraph, point (b)				
124	(b) recommend a relevant audit service to carry out an audit.	(b) recommend request a relevant audit service to carry out an audit.;	(b) recommend a relevant audit service to carry out an audit. issue, in particular:	
Article 11, first paragraph, point (i)				
124a			(i) a recommendation that an audit of a Union entity be carried out;	
Article 11, first paragraph, point (ii)				
124b			(ii) a request that an audit be performed by a third party audit service.	

PUBLIC



124c		All warnings and recommendations shall be directed to the highest level of management of the Union entity concerned.		
Article 11, first paragraph, point (c)				
124d		(ba) inform the Court of Auditors of the alleged non-compliance.		
Article 11, first paragraph, point (c)				
124e			(c) request the Union entity to bring the management, governance and control of cybersecurity risks into compliance with the provisions of this Regulation, where appropriate in a specified manner and within a specified period.	
Article 11, first paragraph, point (d)				
124f			(d) issue an advisory to all Member States and Union entities recommending	

			temporary suspension of data flows to the Union entity.	
Article 11, third paragraph				
124g		2. Where the small Union entities notify that they are unable to meet the deadlines set out in Articles 4(1) and 5(1), the IICB may, in exceptional cases, authorise their extension and set the deadlines for the compliance.		
Article 11, third paragraph				
124h			3. Where the IICB has adopted measures under paragraph 2 points (a) - (d), the Union entity concerned shall provide a detailed account of the measures and actions taken to address the alleged shortcomings identified by the IICB. The Union entity shall submit this account within a reasonable period to be agreed with the IICB.	
Article 11, fourth paragraph				
124i			4. Where the IICB considers that there is a continuous breach of the provisions of this	

			<p>Regulation by a Union entity resulting directly from actions or omissions of an official or other servant of the Union, including at the highest level of management, the IICB shall request the entity concerned to take the appropriate actions, including of disciplinary nature, in accordance, in particular, with the rules laid down in the Staff Regulations and the Conditions of employment of other servants of the European Union. For this purpose, the IICB shall transfer the necessary information to the entity concerned.</p>	
--	--	--	---	--

Chapter IV

125	Chapter IV CERT-EU	Chapter IV CERT-EU	Chapter IV CERT-EU	Chapter IV CERT-EU Text Origin: Commission Proposal
-----	-----------------------	-----------------------	-----------------------	--

Article 12

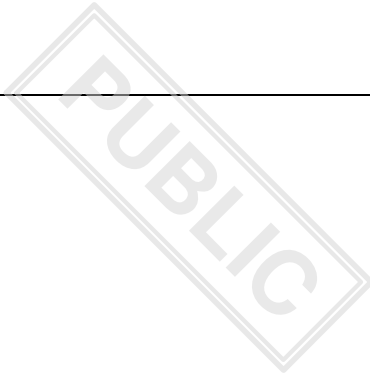
126	Article 12 CERT-EU mission and tasks	Article 12 CERT-EU mission and tasks	Article 12 CERT-EU mission and tasks	Article 12 CERT-EU mission and tasks Text Origin: Commission Proposal
-----	---	---	---	--

Article 12(1)				
127	1. The mission of CERT-EU, the autonomous interinstitutional Cybersecurity Centre for all Union institutions, bodies and agencies, shall be to contribute to the security of the unclassified IT environment of all Union institutions, bodies and agencies by advising them on cybersecurity, by helping them to prevent, detect, mitigate and respond to incidents and by acting as their cybersecurity information exchange and incident response coordination hub.	1. The mission of CERT-EU, the autonomous interinstitutional Cybersecurity Centre for all Union institutions, bodies and agencies entities , shall be to contribute to the security of the unclassified FI ICT environment of all Union institutions, bodies and agencies entities and providing for them services that are analogous to CSIRTs established by the Member States under Directive (EU) 2022/2555, in particular by advising them on cybersecurity, by helping them to prevent, detect, handle , mitigate and , respond to and recover from incidents and by acting as their cybersecurity information exchange and incident response coordination hub.	1. The mission of CERT-EU, the autonomous interinstitutional Cybersecurity Centre for all Union institutions, bodies and agencies; CERT-EU's mission shall be to contribute to the security of the unclassified IT environment of all Union institutions, bodies and agencies entities by advising them on cybersecurity, by helping them to prevent, detect, mitigate and respond to incidents and by acting as their cybersecurity information exchange and incident response coordination hub.	
127a			1a. CERT-EU shall collect, manage, analyse and share information with the Union entities on threats, vulnerabilities and incidents on unclassified ICT infrastructure. It shall coordinate responses to incidents at inter-institutional and Union	

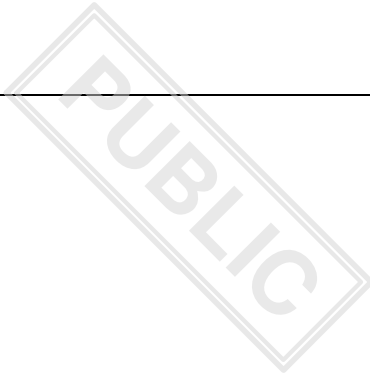
			entity level, including by providing or coordinating the provision of specialised operational assistance.	
Article 12(2)				
128	2. CERT-EU shall perform the following tasks for the Union institutions, bodies and agencies:	2. CERT-EU shall perform the following tasks for the Union institutions, bodies and agencies entities :	2. CERT-EU shall perform the following tasks for the Union institutions, bodies and agencies entities :	
Article 12(2), point (a)				
129	(a) support them with the implementation of this Regulation and contribute to the coordination of the application of this Regulation through the measures listed in Article 13.1 or through ad-hoc reports requested by the IICB;	(a) support them with the implementation of this Regulation and contribute to the coordination of the application of this Regulation through the measures listed in Article 13.1 13(1) or through ad-hoc reports requested by the IICB;	(a) support them with the implementation of this Regulation and contribute to the coordination of the application of this Regulation through the measures provisions listed in Article 13.1 13(1) or through ad-hoc reports requested by the IICB;	
Article 12(2), point (b)				
130	(b) support them with a package of cybersecurity services described in its service catalogue ('baseline services');	(b) support them with a package of cybersecurity services described in its service catalogue ('baseline services');	(b) support them with offer standard CSIRT services for all Union entities through a package of cybersecurity services described in its service catalogue ('baseline services');	

130a		(ba) operate for Union entities who do not have capacity to do it on their own a broad-spectrum Security Operations Centre (SOC) which monitors networks, including first-line 24/7 monitoring for high-severity threats;	PUBLIC	
Article 12(2), point (c)				
131	(c) maintain a network of peers and partners to support the services as outlined in Articles 16 and 17;	(c) maintain a network of peers and partners to support the services as outlined in Articles 16 and 17;	(c) maintain a network of peers and partners to support the services as outlined in Articles 16 and 17;	(c) maintain a network of peers and partners to support the services as outlined in Articles 16 and 17; <small>Text Origin: Commission Proposal</small>
Article 12(2), point (d)				
132	(d) raise to the attention of the IICB any issue relating to the implementation of this Regulation and of the implementation of the guidance documents, recommendations and calls for action;	(d) raise to the attention of the IICB any issue relating to the implementation of this Regulation and of the implementation of the guidance documents, recommendations and calls for action Article 13 and submit proposals for recommendations;	(d) raise to the attention of the IICB any issue relating to the implementation of this Regulation and of the implementation of the guidance documents, recommendations and calls for action;	

Article 12(2), point (e)				
133	(e) report on the cyber threats faced by the Union institutions, bodies and agencies and contribute to the EU cyber situational awareness.	(e) report to the Union entities on the relevant cyber threats faced by and contribute to the Union institutions, bodies and agencies and contribute cyber situational awareness, taking into account the opinion of ENISA, and submit such reports to the IICB, to the CSIRT network referred to in Article 15 of Directive (EU) 2022/2555 and to the EU Intelligence and Situation Centre (EU-INTCEN); EU cyber situational awareness.	(e) report on the cyber threats faced by the Union institutions, bodies and agencies and basis of the information referred to in paragraph 1a, contribute to the EU cyber situational awareness in close cooperation with ENISA. Such information shall be shared with the IICB, as well as the CSIRTs Network and EU-INTCEN;	
Article 12(2), point (f)				
133a		(ea) act as the designated coordinator for the Union entities, for the purpose of coordinated vulnerability disclosure to the European vulnerability database referred to in Article 12 of Directive (EU) 2022/2555;	(f) act as the equivalent of the designated coordinator for the Union entities, as referred to in Article 6 of Directive [proposal NIS 2].	

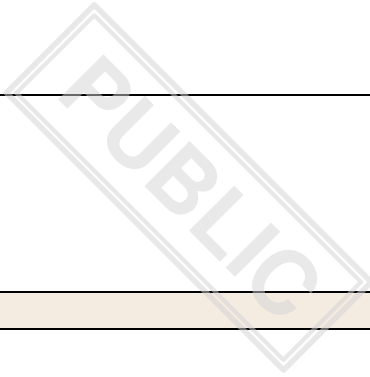


133b		(eb) propose to the IICB, after consulting ENISA, the security criteria, a list of possible KPIs, and scale in the cybersecurity frameworks used by the Union entities;		
133c		(ec) propose to the IICB and prioritise, after consulting ENISA, the cybersecurity domains and the cybersecurity measures that Union entities are to take into account in their cybersecurity framework;		
133d		(ed) provide the Union entities with one or more cybersecurity maturity models, which are to be used in their cybersecurity frameworks and which reflect their size and the cybersecurity domains that they use;		



133e		(ee) provide services that support, with a high level of transparency and reliability, information exchanges, in particular with regard to the Union entities' notifications to CERT-EU;		
Article 12(3)				
133f		(ef) conduct regular risk analysis of the interconnectivity among the Union entities in support of the IICB tasks.		
Article 12(3)				
134	3. CERT-EU shall contribute to the Joint Cyber Unit, built in accordance with the Commission Recommendation of 23 June 2021, including in the following areas:	3. CERT-EU shall contribute to the Joint Cyber Unit, built in accordance with the Commission Recommendation of 23 June 2021, including in the following areas:	<i>deleted</i>	
Article 12(3), point (a)				
135	(a) preparedness, incident coordination, information exchange and crisis response at the technical level on cases linked to	(a) preparedness, incident coordination, information exchange and crisis response at the technical level on cases linked to	<i>deleted</i>	

	Union institutions, bodies and agencies;	Union institutions, bodies and agencies entities;		
<i>Article 12(3), point (b)</i>				
136	(b) operational cooperation regarding the computer security incident response teams (CSIRTs) network, including on mutual assistance, and the broader cybersecurity community;	(b) operational cooperation regarding the computer security incident response teams (CSIRTs) network, including on mutual assistance, and the broader cybersecurity community;	<i>deleted</i>	
136a		(ba) coordination of the management of major incidents and crises at operational level and regular exchange of relevant information among Member States and Union entities within the European cyber crises liaison organisation network (EU-CyCLONe);		
<i>Article 12(3), point (c)</i>				
137	(c) cyber threat intelligence, including situational awareness;	(c) cyber threat intelligence, including situational awareness;	<i>deleted</i>	




137a		(ca) proactive scanning of network and information systems;		
Article 12(3), point (d)				
138	(d) on any topic requiring CERT-EU's technical cybersecurity expertise.	(d) on any topic requiring CERT-EU's technical cybersecurity expertise.	<i>deleted</i>	
Article 12(4)				
139	4. CERT-EU shall engage in structured cooperation with the European Union Agency for Cybersecurity on capacity building, operational cooperation and long-term strategic analyses of cyber threats in accordance with Regulation (EU) 2019/881 of the European Parliament and of the Council.	4. CERT-EU shall engage in structured cooperation with the European Union Agency for Cybersecurity ENISA on capacity building, operational cooperation and long-term strategic analyses of cyber threats in accordance with Regulation (EU) 2019/881. CERT-EU may cooperate and exchange information with Europol's European Cybercrime Centre of the European Parliament and of the Council.	4. Within the framework of competences, CERT-EU shall engage in structured cooperation with the European Union Agency for Cybersecurity ENISA on capacity building, operational cooperation and long-term strategic analyses of cyber threats in accordance with Regulation (EU) 2019/881 of the European Parliament and of the Council.	

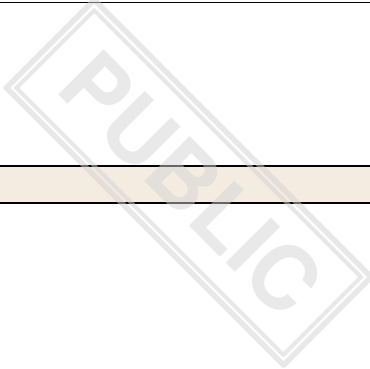
Article 12(5)				
140	5. CERT-EU may provide the following services not described in its service catalogue ('chargeable services'):	5. CERT-EU may provide to the Union entities the following services not described in its service catalogue ('chargeable services'):	5. CERT-EU may provide the following services not described in its service catalogue ('chargeable services'):	
Article 12(5), point (a)				
141	(a) services that support the cybersecurity of Union institutions, bodies and agencies' IT environment, other than those referred to in paragraph 2, on the basis of service level agreements and subject to available resources;	(a) services that support the cybersecurity of Union institutions, bodies and agencies' entities' ICT environment, other than those referred to in paragraph 2, on the basis of service level agreements and subject to available resources, including, via its Security Operations Centre referred to in paragraph 2, point (ba), monitoring of the networks and first-line 24/7 monitoring for high-severity threats for larger Union entities;	(a) services that support the cybersecurity of Union institutions, bodies and agencies' entities' IT environment, other than those referred to in paragraph 2, on the basis of service level agreements and subject to available resources;	
Article 12(5), point (b)				
142	(b) services that support cybersecurity operations or projects of Union institutions, bodies and agencies, other than	(b) services that support cybersecurity operations or projects of Union institutions, bodies and agencies' entities , other	(b) services that support cybersecurity operations or projects of Union institutions, bodies and agencies' entities , other	

	those to protect their IT environment, on the basis of written agreements and with the prior approval of the IICB;	than those to protect their FI ICT environment, on the basis of written agreements and with the prior approval of the IICB;	than those to protect their IT environment, on the basis of written agreements and with the prior approval of the IICB;	
Article 12(5), point (c)				
143	(c) services that support the security of their IT environment to organisations other than the Union institutions, bodies and agencies that cooperate closely with Union institutions, bodies and agencies, for instance by having assigned tasks or responsibilities under Union law, on the basis of written agreements and with the prior approval of the IICB.	(c) services that support the security of their FI ICT environment to organisations other than the Union institutions, bodies and agencies entities that cooperate closely with Union institutions, bodies and agencies entities , for instance by having assigned tasks or responsibilities under Union law, on the basis of written agreements and with the prior approval of the IICB.	(c) services that support the security of their IT environment to organisations other than the Union institutions, bodies and agencies entities that cooperate closely with Union institutions, bodies and agencies entities , for instance by having assigned tasks or responsibilities under Union law, on the basis of written agreements and with the prior approval of the IICB.	
Article 12(6)				
144	6. CERT-EU may organise cybersecurity exercises or recommend participation in existing exercises, in close cooperation with the European Union Agency for Cybersecurity whenever applicable, to test the level of cybersecurity of the Union institutions, bodies and agencies.	6. CERT-EU may shall organise cybersecurity exercises or recommend participation in existing exercises, in close cooperation with the European Union Agency for Cybersecurity ENISA whenever applicable, to test the level of cybersecurity of the Union institutions, bodies and agencies entities on a regular	6. CERT-EU may organise or participate in cybersecurity exercises or recommend participation in existing exercises, in close cooperation with the European Union Agency for Cybersecurity ENISA whenever applicable, to test the level of cybersecurity of the Union institutions, bodies and agencies entities .	

		basis.		
Article 12(7)				
145	7. CERT-EU may provide assistance to Union institutions, bodies and agencies regarding incidents in classified IT environments if it is explicitly requested to do so by the constituent concerned.	7. CERT-EU may shall provide assistance to Union institutions, bodies and agencies entities regarding incidents in classified IT ICT environments if it is explicitly requested to do so by the constituent concerned. The provisions and obligations on all Union entities set out in Chapter V shall not apply to incidents in classified ICT environments unless an individual Union entity explicitly and voluntarily apply them in order to seek actionable assistance from CERT-EU or otherwise contribute to situational awareness at Union level.	7. CERT-EU may provide assistance to Union institutions, bodies and agencies entities regarding incidents in classified IT environments if it is explicitly requested to do so by the constituent Union entities concerned in accordance with their respective procedures. In this case the provisions set out in Articles 19 to 21 of this Regulation shall not apply. Providing an assistance by CERT-EU under this paragraph shall be without prejudice to applicable Member State or Union rules concerning protection of sensitive or classified information.	
Article 12(8)				
145a			8. CERT-EU shall inform Union entities about its incident handling procedures and processes.	

145b		7a. CERT-EU shall submit, under appropriate confidentiality conditions, a yearly report of its activities to the European Parliament. That report shall include relevant and precise information about the major incidents and the way they were dealt with.		
Article 12(9)				
145c			9. CERT-EU may monitor Union entities' network traffic with the consent of the relevant Union entity.	
Article 12(9)				
145d		7b. CERT-EU shall cooperate with the EDPS to support Union entities in incidents entailing a personal data breach as defined in Article 3, point (16), of Regulation (EU) 2018/1725.	11. CERT-EU shall, in cooperation with the European Data Protection Supervisor, support the Union entities concerned when addressing incidents resulting in personal data breaches.	
Article 12(10)				
145e			10. CERT-EU may, if expressly requested by Union entities'	

			policy departments, provide technical advice or input on relevant policy matters.	
145f		7c. The processing of personal data carried out by CERT-EU under this Regulation shall be subject to Regulation (EU) 2018/1725.		
145g		7d. CERT-EU may provide assistance to Union entities regarding the implementation of appropriate cybersecurity cooperation between them in terms of cybersecurity knowledge, staff and ICT resources, and cybersecurity expertise.		
145h		7e. CERT-EU shall inform the EDPS when addressing significant vulnerabilities, significant incidents or major incidents that have the potential to result in personal data		



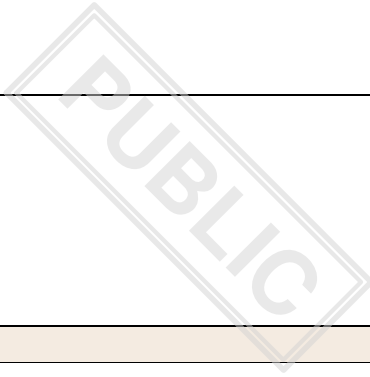
		breaches and/or in the breach of confidentiality of electronic communications.		
145i		7f. CERT-EU shall inform the EDPS about preventive cybersecurity activities that would result in the collection of personal data.		
Article 13				
146	Article 13 Guidance documents, recommendations and calls for action	Article 13 Guidance documents, recommendations and calls for action	Article 13 Guidance documents, recommendations and calls for action	Article 13 Guidance documents, recommendations and calls for action <small>Text Origin: Commission Proposal</small>
Article 13(1)				
147	1. CERT-EU shall support the implementation of this Regulation by issuing:	1. CERT-EU shall support the implementation of this Regulation by issuing:	1. CERT-EU shall support the implementation of this Regulation by issuing:	1. CERT-EU shall support the implementation of this Regulation by issuing: <small>Text Origin: Commission Proposal</small>
Article 13(1), point (a)				

148	(a) calls for action describing urgent security measures that Union institutions, bodies and agencies are urged to take within a set timeframe;	(a) calls for action describing urgent security measures that Union institutions, bodies and agencies entities are urged to take within a set timeframe;	(a) calls for action describing urgent security measures that Union institutions, bodies and agencies entities are urged to take within a set timeframe. Without undue delay after receiving the call for action the concerned Union entity shall inform CERT-EU of how those measures were applied;	
Article 13(1), point (b)				
149	(b) proposals to the IICB for guidance documents addressed to all or a subset of the Union institutions, bodies and agencies;	(b) proposals to the IICB for guidance documents addressed to all or a subset of the Union institutions, bodies and agencies entities ;	(b) proposals to the IICB for guidance documents addressed to all or a subset of the Union institutions, bodies and agencies entities ;	
Article 13(1), point (c)				
150	(c) proposals to the IICB for recommendations addressed to individual Union institutions, bodies and agencies.	(c) proposals to the IICB for recommendations addressed to individual Union institutions, bodies and agencies or all Union entities .	(c) proposals to the IICB for recommendations addressed to individual Union institutions, bodies and agencies entities .	
Article 13(2)				
151	2. Guidance documents and recommendations may include:	2. Guidance documents and recommendations may include:	2. Guidance documents and recommendations may include:	2. Guidance documents and recommendations may include:

PUBLIC

Text Origin: Commission
Proposal

Article 13(2), point (a)				
152	(a) modalities for or improvements to cybersecurity risk management and the cybersecurity baseline;	(a) modalities for or improvements to cybersecurity risk management and the cybersecurity baseline risk-management measures;	(a) modalities for or improvements to cybersecurity risk management and the cybersecurity baseline risk management measures;	
Article 13(2), point (b)				
153	(b) modalities for maturity assessments and cybersecurity plans; and	(b) modalities for arrangements for cybersecurity maturity assessments and cybersecurity plans; and	(b) modalities for maturity assessments and cybersecurity plans; and	
Article 13(2), point (c)				
154	(c) where appropriate, the use of common technology, architecture and associated best practices with the aim of achieving interoperability and common standards within the meaning of Article 4(10) of Directive [proposal NIS 2].	(c) where appropriate, the use of common technology, open-source architecture and associated best practices with the aim of achieving interoperability and common standards within the meaning of Article 4(10) of Directive [proposal NIS 2]. ;	(c) where appropriate, the use of common technology, architecture and associated best practices with the aim of achieving interoperability and common standards, including a coordinated approach to supply chain security within the meaning of Article 4(10) of Directive [proposal NIS 2].	




154a		(ca) where appropriate, facilitate the common purchasing of relevant ICT services and ICT products.		
Article 13(3)				
155	3. The IICB may adopt guidance documents or recommendations on proposal of CERT-EU.	<i>deleted</i>	<i>deleted</i>	
Article 13(4)				
156	4. The IICB may instruct CERT-EU to issue, withdraw or modify a proposal for guidance documents or recommendations, or a call for action.	<i>deleted</i>	<i>deleted</i>	
Article 14				
157	Article 14 Head of CERT-EU	Article 14 Head of CERT-EU	Article 14 Head of CERT-EU	Article 14 Head of CERT-EU Text Origin: Commission Proposal

Article 14, first paragraph				
157a		<p>The Commission, after obtaining the approval of a majority of two thirds of the IICB members, shall appoint the head of CERT-EU. The IICB shall be consulted at all stages of the procedure prior to the appointment of the head of CERT-EU, in particular in drafting vacancy notices, examining applications and appointing selection boards in relation to that post. The final list of candidates shall include at least one man and one woman.</p>	<p>1. The Commission, after having obtained the approval by two-thirds of the members of the IICB, shall appoint the Head of CERT-EU. The IICB shall be consulted at all stages of the procedure prior to the appointment of the Head of CERT-EU, in particular in drafting vacancy notices, examining applications and appointing selection boards in relation to this post.</p>	
Article 14, second paragraph				
157b			<p>2. The Head of CERT-EU shall be responsible for the proper functioning of CERT-EU, acting within its remit under the direction of the IICB. He or she shall be responsible for implementing the strategic direction, guidance, objectives and priorities set by the IICB, and for the management of CERT-EU, including of its financial and human resources.</p>	

			He or she shall report regularly to the IICB Chair.	
Article 14, third paragraph				
157c			3. The Head of CERT-EU shall assist the responsible authorising officer by delegation in drafting the annual activity report containing financial and management information, including the results of controls, drawn up in accordance with Article 66(9) of the Financial Regulation, and shall report regularly to him or her on the implementation of measures in respect of which powers have been sub-delegated to him.	
Article 14, fourth paragraph				
157d			4. The Head of CERT-EU shall draw up annually a financial planning of administrative revenue and expenditure for its activities, the annual work programme proposal, CERT-EU 's service catalogue proposal and the revision thereof, the proposal of modalities for service level agreements and the proposal of key performance indicators for	

			<p>CERT-EU to be approved by the IICB in accordance with Article 10.</p> <p>When revising the list of services in CERT-EU's service catalogue, the Head of CERT-EU shall take into account the resources allocated to CERT-EU.</p>	
Article 14, first paragraph				
158	<p>The Head of CERT-EU shall regularly submit reports to the IICB and the IICB Chair on the performance of CERT-EU, financial planning, revenue, implementation of the budget, service level agreements and written agreements entered into, cooperation with counterparts and partners, and missions undertaken by staff, including the reports referred to in Article 10(1).</p>	<p>The head of CERT-EU shall regularly submit reports at least once a year to the IICB and the IICB Chair on the activities and performance of CERT-EU; financial planning, revenue during the reference period, including on the implementation of the budget, service level agreements and written agreements entered into, cooperation with counterparts and partners, and missions undertaken by staff, including the reports referred to in Article 10(1)10. Those reports shall include the work programme for the next period, financial planning of revenue and expenditure, including staffing, planned updates of CERT-EU's service catalogue and an assessment of the expected impact that such updates may</p>	<p>5. The Head of CERT-EU shall submit annual regularly submit reports to the IICB and the IICB Chair on the performance of CERT-EU, financial planning, revenue, implementation of the budget, service level agreements and written agreements entered into, cooperation with counterparts and partners, and missions undertaken by staff, including the reports referred to in Article 10(1)10(a).</p>	

		have in terms of financial and human resources.		
158a		<i>The head of CERT-EU shall also submit, ad-hoc reports to the IICB upon its request.</i>		
Article 15				
159	Article 15 Financial and staffing matters	Article 15 Financial and staffing matters	Article 15 Financial and staffing matters	Article 15 Financial and staffing matters Text Origin: Commission Proposal
Article 15(1)				
160	1. The Commission, after having obtained the unanimous approval of the IICB, shall appoint the Head of CERT-EU. The IICB shall be consulted at all stages of the procedure prior to the appointment of the Head of CERT-EU, in particular in drafting vacancy notices, examining applications and appointing selection boards in relation to this post.	1. The Commission, after having obtained the unanimous approval of the IICB, shall appoint the Head of CERT-EU. The IICB shall be consulted at all stages of the procedure prior to the appointment of the Head CERT-EU is an autonomous interinstitutional service provider for all Union entities, integrated into the administrative structure of a Commission Directorate-General in order to benefit from the Commission's administrative,	<i>deleted</i>	

		<p>financial, management and accounting support structures. The Commission shall inform the IICB about the administrative location of CERT-EU and any changes thereto. This approach is to be evaluated on a regular basis, in order to allow appropriate action to be taken, including the possible establishment of CERT-EU as a Union office, in particular in drafting vacancy notices, examining applications and appointing selection boards in relation to this post.</p>		
160a			<p>1a. While established as an autonomous interinstitutional service provider for all Union entities, CERT-EU shall be integrated into the administrative structure of a Commission directorate-general in order to benefit from the Commission's administrative, financial management and accounting support structures. The Commission shall inform the IICB about the administrative location of CERT-EU and any changes thereto. This approach</p>	

			shall be evaluated on a regular basis, at the latest before the end of any multiannual financial framework established in accordance with Article 312 TFEU to allow for appropriate action to be taken.	
160b		1a. All decisions related to staffing and budget allocation of the CERT-EU shall be submitted to the formal approval of the IICB.		
Article 15(2)				
161	2. For the application of administrative and financial procedures, the Head of CERT-EU shall act under the authority of the Commission.	2. For the application of administrative and financial procedures, the head of CERT-EU shall act under the authority of the Commission under the supervision of the IICB.	2. For the application of administrative and financial procedures, the Head of CERT-EU shall act under the authority of the Commission.	
Article 15(3)				
162	3. CERT-EU tasks and activities, including services provided by CERT-EU pursuant to Article 12(2), (3), (4), (6), and Article 13(1) to Union institutions, bodies	3. CERT-EU tasks and activities, including services provided by CERT-EU pursuant to Article 12(2), (3), (4), (6), and Article 13(1) to Union institutions, bodies	3. CERT-EU tasks and activities, including services provided by CERT-EU pursuant to Article 12(2), (3) , (4), (6), and Article 13(1) to Union institutions, bodies	

	and agencies financed from the heading of the multiannual financial framework dedicated to European public administration, shall be funded through a distinct budget line of the Commission budget. CERT-EU earmarked posts shall be detailed in a footnote to the Commission establishment plan.	and agencies entities financed from the heading of the multiannual financial framework dedicated to European public administration, shall be funded through a distinct budget line of the Commission budget. CERT-EU earmarked posts shall be detailed in a footnote to the Commission establishment plan.	and agencies entities financed from the heading of the multiannual financial framework dedicated to European public administration, shall be funded through a distinct budget line of the Commission budget. CERT-EU earmarked posts shall be detailed in a footnote to the Commission establishment plan.	
Article 15(4)				
163	4. Union institutions, bodies and agencies other than those referred to in paragraph 3 shall make an annual financial contribution to CERT-EU to cover the services provided by CERT-EU pursuant to that paragraph 3. The respective contributions shall be based on orientations given by the IICB and agreed between each entity and CERT-EU in service level agreements. The contributions shall represent a fair and proportionate share of the total costs of services provided. They shall be received by the distinct budget line referred to in paragraph 3 as assigned revenue as provided for in Article 21(3), point (c) of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the	4. Union institutions, bodies and agencies entities other than those referred to in paragraph 3 shall make an annual financial contribution to CERT-EU to cover the services provided by CERT-EU pursuant to that paragraph 3. The respective contributions shall be based on orientations given by the IICB and agreed between each entity and CERT-EU in service level agreements. The contributions shall represent a fair and proportionate share of the total costs of services provided. They shall be received by the distinct budget line referred to in paragraph 3 as assigned revenue as provided for in Article 21(3), point (c) of Regulation (EU, Euratom) 2018/1046 of the European	4. Union institutions, bodies and agencies entities other than those referred to in paragraph 3 shall make an annual financial contribution to CERT-EU to cover the services provided by CERT-EU pursuant to that paragraph 3. The respective contributions shall be based on orientations given by the IICB and agreed between each entity and CERT-EU in service level agreements. The contributions shall represent a fair and proportionate share of the total costs of services provided. They shall be received by the distinct budget line referred to in paragraph 3 as assigned revenue as provided for in Article 21(3), point (c) of Regulation (EU, Euratom) 2018/1046 of the European	

	<p>Council¹.</p> <p>1. Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 (OJ L 193, 30.7.2018, p. 1).</p>	<p>Parliament and of the Council¹.</p> <p>1. Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 (OJ L 193, 30.7.2018, p. 1).</p>	<p>Parliament and of the Council¹⁶.</p> <p>1. Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 (OJ L 193, 30.7.2018, p. 1).</p> <p>6. Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 (OJ L 193, 30.7.2018, p. 1).</p>	
Article 15(5)				
164	<p>5. The costs of the tasks defined in Article 12(5) shall be recovered from the Union institutions, bodies and agencies receiving the CERT-EU services. The revenues shall be assigned to the budget lines supporting the costs.</p>	<p>5. The costs of the tasks defined in Article 12(5) shall be recovered from the Union institutions, bodies and agenciesentities receiving the CERT-EU services. The revenues shall be assigned to the budget lines supporting the costs.</p>	<p>5. The costs of the tasks defined in Article 12(5) shall be recovered from the Union institutions, bodies and agenciesentities receiving the CERT-EU services. The revenues shall be assigned to the budget lines supporting the costs.</p>	
Article 16				

165	Article 16 Cooperation of CERT-EU with Member State counterparts	Article 16 Cooperation of CERT-EU with Member State counterparts	Article 16 Cooperation of CERT-EU with Member State counterparts	Article 16 Cooperation of CERT-EU with Member State counterparts Text Origin: Commission Proposal
Article 16(1)				
166	1. CERT-EU shall cooperate and exchange information with national counterparts in the Member States, including CERTs, National Cybersecurity Centres, CSIRTs, and single points of contact referred to in Article 8 of Directive [proposal NIS 2], on cyber threats, vulnerabilities and incidents, on possible countermeasures and on all matters relevant for improving the protection of the IT environments of Union institutions, bodies and agencies, including through the CSIRTs network referred to in Article 13 of Directive [proposal NIS 2].	1. CERT-EU shall cooperate and exchange information with national counterparts in the Member States, including CERTs, National Cybersecurity Centres, CSIRTs, and single points of contact referred to in Article 8 of Directive [proposal NIS 2](EU) 2022/2555, on cyber threats, vulnerabilities and incidents, on near misses, possible countermeasures as well as best practices and on all matters relevant for improving the protection of the ICT environments of Union institutions, bodies and agencies entities , including through the CSIRTs network referred to in Article 13 15 of Directive [proposal NIS 2](EU) 2022/2555. CERT-EU shall support the Commission in the EU-CyCLONe referred to in Article 16 of Directive (EU) 2022/2555 on coordinated	1. CERT-EU shall without undue delay cooperate and exchange information with national counterparts in the Member States, including CERTs, National Cybersecurity Centres, CSIRTs, notably, CSIRTs referred to in Article 9 of Directive [proposal NIS 2], and/or where applicable national competent authorities and single points of contact referred to in Article 8 of Directive [proposal NIS 2], on cyber threats, vulnerabilities and incidents, on possible countermeasures and on all matters relevant for improving the protection of the IT environments of Union institutions, bodies and agencies entities , including through the CSIRTs network referred to in Article 13 of Directive [proposal NIS 2].	

		management of major incidents and crises.		

PUBLIC

166a			<p>1a. CERT-EU shall, without delay, notify any relevant national counterparts referred to in paragraph 1 in a Member State, when it becomes aware of significant incidents occurring within the territory of that Member State, unless CERT-EU has the information that the affected Union entity has already reported such incident in accordance with Article 20(2a).</p>	
Article 16(2)				
167	<p>2. CERT-EU may exchange incident-specific information with national counterparts in the Member States to facilitate detection of similar cyber threats or incidents without the consent of the affected constituent. CERT-EU may only exchange incident-specific information which reveals the identity of the target of the cybersecurity incident with the consent of the affected constituent.</p>	<p>2. CERT-EU may exchange incident-specific information with national counterparts in the Member States to facilitate detection of similar cyber threats or incidents without the consent authorisation of the constituent affected, provided that personal data is protected in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council¹ constituent. CERT-EU may only exchange incident-specific information which reveals the</p>	<p>2. CERT-EU may shall without undue delay exchange incident-specific information with national counterparts in the Member States to facilitate detection of similar cyber threats or incidents or to contribute to the analysis of an incident without needing the consent of the affected constituent Union entity . CERT-EU may only shall not exchange incident-specific information which reveals the identity of the target of the cybersecurity incident with the consent of the affected</p>	

		<p>identity of the target of the cybersecurity incident with the consent authorisation of the constituent affected constituent and in compliance with Regulation (EU) 2016/679.</p> <p><u>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).</u></p>	<p>constituent unless</p>	
167a			<p>2a. there is consent of the affected Union entity;</p>	
167b			<p>2b. the affected Union entity already published that it was affected;</p>	
167c			<p>2c. there is no consent of the affected Union entity, but the publication of the identity of the affected Union entity would</p>	

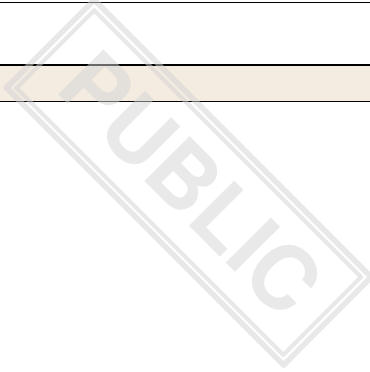
			<p>increase the probability that incidents elsewhere will be avoided or mitigated. Such decisions require the approval of the Head of CERT-EU. The affected Union entity shall be informed before the publication.</p>	
Article 17				
168	<p>Article 17 Cooperation of CERT-EU with non-Member State counterparts</p>	<p>Article 17 Cooperation of CERT-EU with non-Member State counterparts</p>	<p>Article 17 Cooperation of CERT-EU with non-Member State other counterparts</p>	
Article 17(1)				
169	<p>1. CERT-EU may cooperate with non-Member State counterparts including industry sector-specific counterparts on tools and methods, such as techniques, tactics, procedures and best practices, and on cyber threats and vulnerabilities. For all cooperation with such counterparts, including in frameworks where non-EU counterparts cooperate with national counterparts of Member States, CERT-EU shall seek prior approval from the IICB.</p>	<p>1. CERT-EU may cooperate with non-Member State counterparts that are subject to Union cybersecurity requirements or requirements of similar nature, including industry sector-specific counterparts on tools and methods, such as techniques, tactics, procedures and best practices, and on cyber threats and vulnerabilities. For all cooperation with such counterparts, including in frameworks where non-EU counterparts cooperate with national counterparts of Member States, CERT-EU shall seek prior</p>	<p>1. CERT-EU may cooperate with counterparts in the European Union other than those mentioned in Article 16, non-Member State counterparts including industry sector-specific counterparts on tools and methods, such as techniques, tactics, procedures and best practices, and on cyber threats and vulnerabilities. For all cooperation with such counterparts, CERT-EU shall seek prior approval from the IICB on a case-by-case basis. CERT-EU shall inform any relevant including in</p>	

		approval from the IICB.	frameworks where non-EU counterparts cooperate with national counterparts of Member States, CERT-EU shall seek prior approval from the IICB referred to in Article 16(1), in a Member State in which the counterpart is located, when CERT-EU establishes cooperation with such counterparts.	
Article 17(2)				
170	2. CERT-EU may cooperate with other partners, such as commercial entities, international organisations, non-European Union national entities or individual experts, to gather information on general and specific cyber threats, vulnerabilities and possible countermeasures. For wider cooperation with such partners, CERT-EU shall seek prior approval from the IICB.	2. CERT-EU may cooperate with other partners, such as commercial entities (including industry sector-specific entities) , international organisations, non-European Union national entities or individual experts, to gather information on general and specific cyber threats, near misses , vulnerabilities and possible countermeasures. For wider cooperation with such partners, CERT-EU shall seek prior approval from the IICB.	2. CERT-EU may cooperate with other partners, such as commercial entities, international organisations, non-European Union national entities or individual experts, to gather information on general and specific cyber threats, vulnerabilities and possible countermeasures. For wider cooperation with such partners, CERT-EU shall seek prior approval from the IICB on a case-by-case basis.	
Article 17(3)				
171	3. CERT-EU may, with the consent of the constituent affected by an incident, provide information	3. CERT-EU may, with the consent of the constituent affected by an incident, provide information	3. CERT-EU may, provided a non-disclosure arrangement or contract is in place with the	

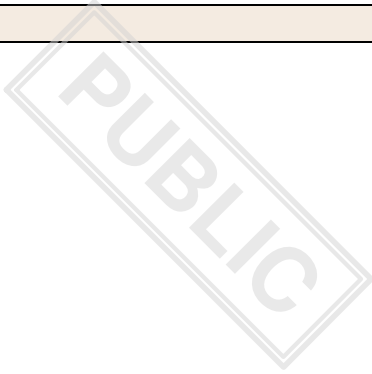
	related to the incident to partners that can contribute to its analysis.	related to the incident to partners that can contribute to its analysis.	relevant partner , with the consent of the constituent Union entity affected by an incident, provide information related to the specific incident to partners that can contribute referred to in paragraphs 1 and 2 solely for the purpose of contributing to its analysis. Such non-disclosure agreements or contracts shall be legally verified in accordance with the relevant internal Commission procedures. Non-disclosure agreements or contracts shall not require prior approval by the IICB, but the chair of the IICB shall be informed.	
Article 17(4)				
171a			4. CERT-EU may exceptionally enter into service level agreements with entities other than the Union entities with the prior approval of the IICB.	
Chapter V				
172	Chapter V COOPERATION AND REPORTING OBLIGATIONS	Chapter V COOPERATION AND REPORTING OBLIGATIONS	Chapter V COOPERATION AND REPORTING OBLIGATIONS	Chapter V COOPERATION AND REPORTING OBLIGATIONS

				Text Origin: Commission Proposal
Article 18				
173	Article 18 Information handling	Article 18 Information handling	Article 18 Information handling	Article 18 Information handling Text Origin: Commission Proposal
Article 18(1)				
174	1. CERT-EU and Union institutions, bodies and agencies shall respect the obligation of professional secrecy in accordance with Article 339 of the Treaty on the Functioning of the European Union or equivalent applicable frameworks.	1. CERT-EU and Union institutions, bodies and agencies entities shall respect the obligation of professional secrecy in accordance with Article 339 of the Treaty on the Functioning of the European Union or equivalent applicable frameworks.	1. CERT-EU and Union institutions, bodies and agencies entities shall respect the obligation of professional secrecy in accordance with Article 339 of the Treaty on the Functioning of the European Union or equivalent applicable frameworks.	
Article 18(2)				
175	2. The provisions of Regulation (EC) No 1049/2001 of the European Parliament and the Council ¹ shall apply with regard to requests for public access to documents held by CERT-EU, including the obligation under that Regulation to consult other Union institutions, bodies and agencies	2. The provisions of Regulation (EC) No 1049/2001 of the European Parliament and the Council ¹ shall apply with regard to requests for public access to documents held by CERT-EU, including the obligation under that Regulation to consult other Union institutions, bodies and	2. The provisions of Regulation (EC) No 1049/2001 of the European Parliament and the Council ¹⁷ shall apply with regard to requests for public access to documents held by CERT-EU, including the obligation under that Regulation to consult other Union institutions, bodies and	

	<p>whenever a request concerns their documents.</p> <p>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).</p>	<p>agencies entities, or, where relevant, Member States, whenever a request concerns their documents.</p> <p>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).</p>	<p>agencies entities, and where relevant the Member States, whenever a request concerns their documents.</p> <p>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).</p> <p>7. 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).</p>	
Article 18(3)				
176	<p>3. The processing of personal data carried out under this Regulation shall be subject to Regulation (EU) 2018/1725 of the European Parliament and of the Council.</p>	<p>3. The processing of personal data carried out under this Regulation shall be subject to Regulation (EU) 2018/1725.</p> <p>Any processing, exchange, collection or retention of personal data by CERT-EU, the IICB and Union entities shall be limited to processing, exchange, collection or retention that is strictly necessary and shall be carried out for the sole purpose of fulfilling their respective obligations under this Regulation of the European Parliament and of the Council.</p>	<i>deleted</i>	

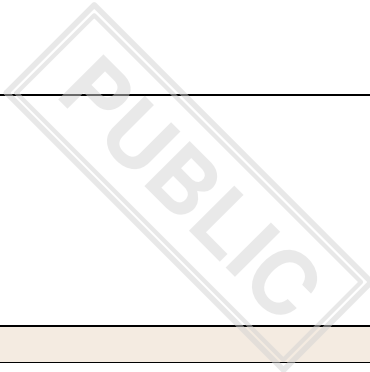


176a		<p>3a. The Commission shall, by ... [one year after the date of entry into force of this Regulation], adopt a delegated act in accordance with Article 24a to specify which personal data processing activities are permitted under this Regulation, including the purpose of the processing, the categories of personal data, the categories of data subjects, the conditions for data processing, maximum retention periods, the definition of the data controllers and processors and recipients in the case of transmission.</p>		
176b		<p>The delegated act referred to in the first subparagraph shall limit processing activities to those that are strictly necessary and shall require that such processing activities be as targeted as possible and do not include the indiscriminate retention of traffic or content data.</p>		

176c		The Commission shall amend the delegated act referred to in the first subparagraph where it identifies significant changes with regard to the necessity or specific purposes, or to the entities involved in the processing of personal data for the purposes of this Regulation.		
Article 18(4)				
177	4. The handling of information by CERT-EU and its Union institutions, bodies and agencies shall be in line with the rules laid down in [proposed Regulation on information security].	4. The handling of information by CERT-EU and its Union institutions, bodies and agencies entities shall be in line with the rules laid down in [proposed Regulation on information security]. When cooperating with other counterparts equivalent information handling rules shall be used by the CERT-EU.	4. The handling of information by CERT-EU and its Union institutions, bodies and agencies entities shall be in line with the applicable rules laid down in [proposed Regulation on information security].	
Article 18(5)				
178	5. Any contacts with CERT-EU initiated or sought by national security and intelligence services shall be communicated to the Commission's Security Directorate	5. Any contacts with CERT-EU initiated or sought by national security and intelligence services shall be communicated to the Commission's Security	<i>deleted</i>	

	and the chair of the IICB without undue delay.	Directorate, Europol and the chair of the IICB without undue delay.		

PUBLIC



178a		5a. Information on the completion of security plans by the Union entities shall be shared with the discharge authorities.		
178b		5b. Guidance documents and recommendations, and calls for actions issued by the IICB shall be shared with the discharge authorities.		
Article 19				
179	Article 19 Sharing obligations	Article 19 Cybersecurity information sharing arrangements and obligations	Article 19 Sharing obligations Cybersecurity information sharing	
179a		-1. Union entities may voluntarily notify and provide information to CERT-EU on cyber threats, incidents, near misses and vulnerabilities that affect them. CERT-EU shall ensure that effective measures	-1. Union entities may voluntarily provide CERT-EU with information on cyber threats, incidents, near misses and vulnerabilities affecting them. CERT-EU shall ensure that efficient means of	

		<p>are adopted to ensure the confidentiality and appropriate protection of the information provided by the reporting Union entity. CERT-EU shall ensure that efficient means of communication are available for the purpose of facilitating information sharing with the Union entities. When processing notifications, CERT-EU may prioritise the processing of mandatory notifications over voluntary notifications. Voluntary notification shall not result in the imposition of any additional obligations upon the reporting Union entity to which it would not have been subject had it not submitted the notification.</p>	<p>communication are available for the purpose of facilitating information sharing with the Union entities. CERT-EU may prioritise the processing of mandatory notifications over voluntary notifications.</p>	
Article 19(1)				
180	<p>1. To enable CERT-EU to coordinate vulnerability management and incident response, it may request Union institutions, bodies and agencies to provide it with information from their respective IT system inventories that is relevant for the CERT-EU support. The requested institution, body or agency shall transmit the</p>	<p>1. To enable CERT-EU effectively perform its mission and tasks laid down in Article 12 of this Regulation, in particular to coordinate vulnerability management and incident response, it may request Union institutions, bodies and agencies entities to provide it with information from their respective IT system</p>	<p>1. To perform its mission and tasks as defined in Article 12, CERT-EU enable CERT-EU to coordinate vulnerability management and incident response, it may request Union institutions, bodies and agencies entities to provide it with information from their respective IT system inventories, including</p>	

	<p>requested information, and any subsequent updates thereto, without undue delay.</p>	<p>inventories that is relevant for the CERT-EU support. The requested institution, body or agency shall Union entity may transmit the requested information, and any subsequent updates thereto, without undue delay.</p>	<p>information relating to cyber threats, near misses, vulnerabilities, indicators of compromise, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyber incidents . The requested Union entity that is relevant for the CERT-EU support. The requested institution, body or agency shall transmit the requested information, and any subsequent updates thereto, without undue delay.</p>	
180a		<p>Without prejudice to Regulation (EU) 2018/1725, any sharing of data between CERT-EU and Union entities shall be carried out in line with the principles of clear safeguards for specific use-cases and shall use mutual legal assistance treaties and other agreements, in order to ensure a high level of protection for rights when processing requests for cross-border access to data.</p>		

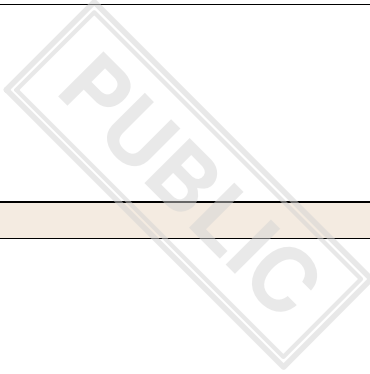
Article 19(2)				
181	2. The Union institutions, bodies and agencies, upon request from CERT-EU and without undue delay, shall provide it with digital information created by the use of electronic devices involved in their respective incidents. CERT-EU may further clarify which types of such digital information it requires for situational awareness and incident response.	<i>deleted</i>	2. The Union institutions, bodies and agencies entities , upon request from CERT-EU and without undue delay, shall provide it with digital information created by the use of electronic devices involved in their respective incidents. CERT-EU may further clarify which types of such digital information it requires for situational awareness and incident response.	
Article 19(3)				
182	3. CERT-EU may only exchange incident-specific information which reveals the identity of the Union institution, body or agency affected by the incident with the consent of that entity. CERT-EU may only exchange incident-specific information which reveals the identity of the target of the cybersecurity incident with the consent of the entity affected by the incident.	3. CERT-EU may only exchange incident-specific information which reveals the identity of the Union institution, body or agency entity affected by the incident with the consent of that entity. CERT-EU may only exchange incident-specific information which reveals the identity of the target of the cybersecurity incident with the consent of the entity affected by the incident. In view of its scrutiny tasks, the European Parliament may request such	3. CERT-EU may only exchange incident-specific information with the Union entities which reveals the identity of the Union institution, body or agency entity affected by the incident with the consent of that entity. CERT-EU may only exchange incident-specific information which reveals the identity of the target of the cybersecurity incident with the consent of the entity affected by the incident. Where consent is withheld, the entity concerned shall provide duly justified	

		<p>information without the consent of the Union entity concerned. Where the European Parliament requests the information without the consent of the entity concerned, its deliberations shall not be held in public and all relevant documents shall be considered only on a need-to-know basis.</p>	<p>reasons to CERT-EU.</p>	
Article 19(4)				
183	<p>4. The sharing obligations shall not extend to EU Classified Information (EUCI) and to information that a Union institution, body or agency has received from a Member State Security or Intelligence Service or law enforcement agency under the explicit condition that it will not be shared with CERT-EU.</p>	<p>4. The cybersecurity information sharing arrangements and obligations shall not extend to EU Classified Information (EUCI) and to information that a Union institution, body or agencyentity has received from a Member State Security or Intelligence Service or law enforcement agency, unless the Member State Security or Intelligence Service or law enforcement agency concerned allow that information to under the explicit condition that it will not be shared with CERT-EU.</p>	<p>4. The sharing obligations shall not extend to EU Classified Information (EUCI) and to information that at the distribution of which beyond the recipient Union institution, body or agency has received from a Member State Security or Intelligence Service or law enforcement agency under the explicit condition that it will notentity has been excluded by the source of the information by means of a visible marking, unless the source of the information explicitly allows this information to be shared with CERT-EU.</p>	
Article 20				
184				

	Article 20 Notification obligations	Article 20 Notification Reporting obligations	Article 20 Notification Reporting obligations	
Article 20(-1)				
184a			-1. An incident shall be considered to be significant if:	
Article 20(-1), first subparagraph a				
184b			(a) it has caused or is capable of causing severe operational disruption to the functioning of the Union entity or financial loss for the Union entity concerned;	
Article 20(-1), first subparagraph b				
184c			(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.	
Article 20(1), first subparagraph				
185	1. All Union institutions, bodies and agencies shall make an initial notification to CERT-EU of significant cyber threats, significant vulnerabilities and significant incidents without undue	1. All Union institutions, bodies and agencies entities shall make an initial notification report to CERT-EU of significant cyber threats, significant vulnerabilities and significant incidents without undue	1. All Union institutions, bodies and agencies entities shall make an initial notification submit to CERT-EU of significant cyber threats, significant vulnerabilities and significant incidents without	

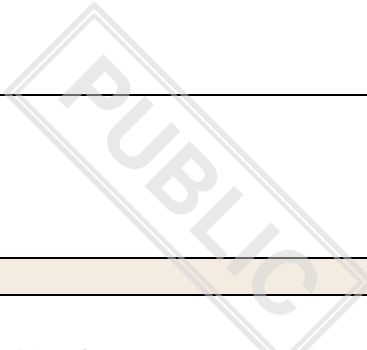
	delay and in any event no later than 24 hours after becoming aware of them.	delay and in any event no later than 24 hours after becoming aware of them in accordance with paragraph 1d any incident that has a significant impact. An incident shall be considered to be significant if:	undue delay and in any event no later than 24 hours after becoming aware of them.:	
185a		(a) it has caused or is capable of causing severe operational disruption of the service or financial losses for the entity concerned;		
185b		(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.		
185c		1a The Union entities shall notify, inter alia, any information enabling the CERT-EU to determine any cross-entities impact, impact on the hosting Member State or cross-border		

		<p>impact following a significant incident. The mere act of notification shall not render the notifying Union entity subject to increased liability.</p>		
185d		<p>1b Where applicable, Union entities shall notify, without undue delay, to the users of the network and information systems affected, or other components of the ICT environment, that are potentially affected by a significant incident or a significant cyber threat of any measures or remedies that can be taken in response to the incident or threat. Where appropriate, Union entities shall inform users of the threat itself.</p>		
185e		<p>1c Where a significant incident or significant cyber threat affects a network and information system, or a component of a Union entity's ICT environment that is knowingly connected with another Union entity's ICT environment, CERT-EU shall notify, without undue delay, the</p>		



		Union entity affected.		

PUBLIC



185f		1d All Union entities shall submit to CERT-EU:		
185g		(a) without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-entity or a cross-border impact;	(a) without undue delay and in any event within 24 hours after having become aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is presumably caused by unlawful or malicious action and has or could have a cross-border impact;	
185h		(b) without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident report, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, its severity and impact, as well as,	(b) without undue delay and in any event within 72 hours after having become aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in subparagraph (a) and indicate an initial assessment of the significant incident, its severity	

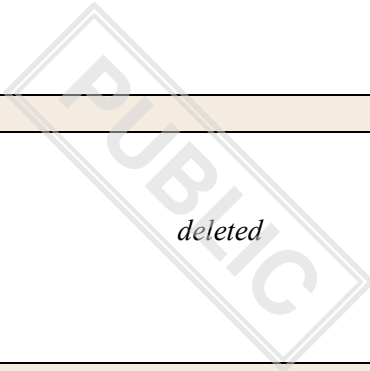
		where available, the indicators of compromise;	and impact, as well as where available, the indicators of compromise;	
185i		(c) upon the request of CERT-EU, an intermediate report on relevant status updates.	(c) upon the request of CERT-EU, an intermediate report on relevant status updates;	
185j			(d) a final report not later than one month after the submission of the significant incident notification under point (b), including at least the following:	
Article 20(1), second subparagraph d (i)				
185k			(i) a detailed description of the significant incident, its severity and impact;	
Article 20(1), second subparagraph d (ii)				
185l			(ii) the type of threat or root cause that likely triggered the significant incident;	

Article 20(1), second subparagraph d (iii)				
185m			(iii) applied and ongoing mitigation measures.	
Article 20(1), second subparagraph d (iv)				
185n			(iv) where applicable, the cross-border impact of the significant incident;	
Article 20(1), second subparagraph e				
185o			(e) in cases of ongoing significant incidents at the time of the submission of the final report referred to in point (d), a progress report at that time and a final report within one month after the incident has been handled.	
Article 20(1), second subparagraph				
186	In duly justified cases and in agreement with CERT-EU, the Union institution, body or agency concerned can deviate from the deadline laid down in the previous	<i>deleted</i>	<i>deleted</i>	

	paragraph.			
Article 20(2)				
187	2. The Union institutions, bodies and agencies shall further notify to CERT-EU without undue delay appropriate technical details of cyber threats, vulnerabilities and incidents that enable detection, incident response or mitigating measures. The notification shall include if available:	2. The Union institutions, bodies and agencies shall further notify to CERT-EU without undue delay appropriate technical details of cyber threats, vulnerabilities and incidents that enable detection, entities shall further submit to CERT-EU a final report, not later than one month after the submission of the incident report, referred to in paragraph 1d, point (b). In cases of ongoing significant incidents at the time of the submission of the final report, a progress report at that time and a final report shall be transmitted within one month after the incident response or mitigating measures. The notification has been handled. The incident report shall include at least the following, if available:	<i>deleted</i>	
Article 20(2), point (a)				
188	(a) relevant indicators of compromise;	(a) relevant indicators of compromise a detailed description of the incident, including its severity and impact;	<i>deleted</i>	

--	--	--	--	--

PUBLIC



<i>Article 20(2), point (b)</i>				
189	(b) relevant detection mechanisms;	(b) relevant detection mechanisms the type of threat or root cause that is likely to have triggered the incident;	<i>deleted</i>	
<i>Article 20(2), point (c)</i>				
190	(c) potential impact;	(c) potential impact the mitigation measures that have been or are being carried out;	<i>deleted</i>	
<i>Article 20(2), point (d)</i>				
191	(d) relevant mitigating measures.	(d) relevant mitigating measures where applicable, the potential impact of the incident on other Union entities or cross-border impact.	<i>deleted</i>	
<i>Article 20(2a)</i>				
191a			2a. All Union entities shall share the information reported in accordance with paragraph 1 within the same timeline with any relevant national counterparts referred to in	

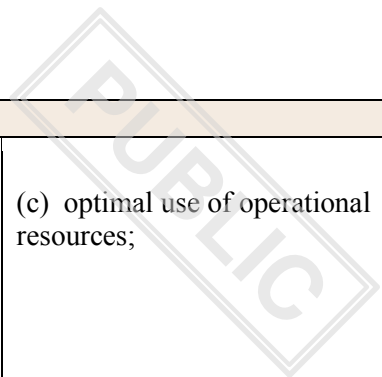
			Article 16(1) where it is located.	
191b		<p>2a. In duly justified cases and in agreement with CERT-EU, the Union entity concerned may derogate from the deadline laid down in paragraph 2. The Union entity concerned shall provide a progress report by the deadline of the submission of a final report, if a derogation is agreed on.</p>		
191c		<p>2b. The Union entities, upon the request of CERT-EU shall without undue delay, provide CERT-EU with digital information created by the use of electronic devices involved in their respective incidents. CERT-EU may further clarify which types of such digital information it requires for situational awareness and incident response.</p>		
Article 20(3)				
192	3. CERT-EU shall submit to ENISA on a monthly basis a	3. CERT-EU shall submit to ENISA on a monthly basis a	3. CERT-EU shall submit to the IICB, the EU INTCEN and the	

	summary report including anonymised and aggregated data on significant cyber threats, significant vulnerabilities and significant incidents notified in accordance with paragraph 1.	summary report including anonymised and aggregated data on significant incidents , cyber threats, significant vulnerabilities and significant incidents incidents, near misses and vulnerabilities notified in accordance with paragraph 1d of this Article and with Article 19(-1)† .	CSIRTs Network every three months ENISA on a monthly basis a summary report including anonymised and aggregated data on significant cyber threats, vulnerabilities in accordance with Article 19, Union entities' replies to calls for action in accordance with Article 13(1), point (a), significant vulnerabilities and significant incidents notified in accordance with paragraph 1. That report shall constitute an input to the biennial report on the state of cybersecurity in the Union under Article 15 of Directive [proposal NIS 2].	
Article 20(4)				
193	4. The IICB may issue guidance documents or recommendations concerning the modalities and content of the notification. CERT-EU shall disseminate the appropriate technical details to enable proactive detection, incident response or mitigating measures by Union institutions, bodies and agencies.	4. By ... [one year after the date of entry into force of the Regulation], the CERT-EU shall The IICB may issue guidance documents or recommendations concerning the modalities and the arrangements relating to, and the content of, the reports. When preparing such guidance documents or recommendations, the CERT-EU shall take into account the specifications made by any implementing acts	4. The IICB may shall, by [6 months after the date of entry into force of this Regulation], issue guidance documents or recommendations concerning further specifying the modalities, format and content of the notification-reporting . The guidance documents or recommendations shall duly take into account the provisions being implemented by any implementing acts according to	

		<p>adopted by the Commission specifying the type of information, the format and the procedure of a the-notification submitted pursuant to Article 23(11) of Directive (EU) 2022/2555. CERT-EU shall disseminate the appropriate technical details to enable proactive detection, incident response or mitigating measures by Union institutions, bodies and agenciesentities.</p>	<p>Article 20(11) of Directive [proposal NIS 2] CERT-EU shall disseminate the appropriate technical details to enable proactive detection, incident response or mitigating measures by Union institutions, bodies and agenciesentities.</p>	
Article 20(5)				
194	<p>5. The notification obligations shall not extend to EUCI and to information that a Union institution, body or agency has received from a Member State Security or Intelligence Service or law enforcement agency under the explicit condition that it will not be shared with CERT-EU.</p>	<p>5. The notificationreporting obligations shall not extend to EUCI and to information that a Union institution, body or agencyentity has received from a Member State Security or Intelligence Service or law enforcement agency, under the explicit condition that it will not be shared with CERT-EU.</p>	<p>5. The notificationreporting obligations shall not extend to EUCI and to information that a Union institution, body or agency has received from a Member State Security or Intelligence Service or law enforcement agency under the explicit condition that it will notthe distribution of which beyond the recipient Union entity has been excluded by the source of the information by means of a visible marking, unless the source of the information explicitly allows this information to be shared with CERT-EU.</p>	

Article 21				
195	Article 21 Incident response coordination and cooperation on significant incidents	Article 21 Incident response coordination and cooperation on significant incidents	Article 21 Incident response coordination and cooperation on significant incidents	
Article 21(1)				
196	1. In acting as a cybersecurity information exchange and incident response coordination hub, CERT-EU shall facilitate information exchange with regards to cyber threats, vulnerabilities and incidents among:	1. In acting as a cybersecurity information exchange and incident response coordination hub, CERT-EU shall facilitate information exchange with regards to cyber threats, vulnerabilities, near misses and incidents among:	1. In acting as a cybersecurity information exchange and incident response coordination hub, CERT-EU shall facilitate information exchange with regards to cyber threats, vulnerabilities and incidents among:	
Article 21(1), point (a)				
197	(a) Union institutions, bodies and agencies;	(a) Union institutions, bodies and agencies entities ;	(a) Union institutions, bodies and agencies entities ;	
Article 21(1), point (b)				
198	(b) the counterparts referred to in Articles 16 and 17.	(b) the counterparts referred to in Articles 16 and 17.	(b) the counterparts referred to in Articles 16 and 17.	(b) the counterparts referred to in Articles 16 and 17. Text Origin: Commission Proposal

Article 21(2)				
199	2. CERT-EU shall facilitate coordination among Union institutions, bodies and agencies on incident response, including:	2. CERT-EU shall facilitate coordination among Union institutions, bodies and agencies entities on incident response, including:	2. CERT-EU, where relevant in close cooperation with ENISA in accordance with Article 7(7)(d) of the Cybersecurity Act⁹ , shall facilitate coordination among Union institutions, bodies and agencies entities on incident response, including:	
			<p>9. 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)</p>	
Article 21(2), point (a)				
200	(a) contribution to consistent external communication;	(a) contribution to consistent external communication;	(a) contribution to consistent external communication;	(a) contribution to consistent external communication; Text Origin: Commission Proposal
Article 21(2), point (b)				
201	(b) mutual assistance;	(b) mutual assistance;	<i>deleted</i>	



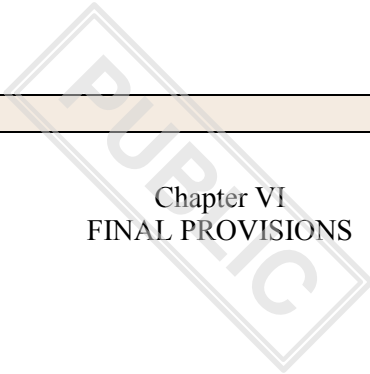
Article 21(2), point (c)				
202	(c) optimal use of operational resources;	(c) optimal use of operational resources;	(c) optimal use of operational resources;	(c) optimal use of operational resources; Text Origin: Commission Proposal
Article 21(2), point (d)				
203	(d) coordination with other crisis response mechanisms at Union level.	(d) coordination with other crisis response mechanisms at Union level.	(d) coordination with other crisis response mechanisms at Union level.	(d) coordination with other crisis response mechanisms at Union level. Text Origin: Commission Proposal
Article 21(3)				
204	3. CERT-EU shall support Union institutions, bodies and agencies regarding situational awareness of cyber threats, vulnerabilities and incidents.	3. CERT-EU, in cooperation with ENISA, shall support Union entities shall support Union institutions, bodies and agencies regarding situational awareness of cyber threats, vulnerabilities, near misses and incidents, as well as sharing the latest developments in the field of cybersecurity.	3. CERT-EU in close cooperation with ENISA shall support Union institutions, bodies and agencies entities regarding situational awareness of cyber threats, vulnerabilities and incidents.	

Article 21(4)				
205	4. The IICB shall issue guidance on incident response coordination and cooperation for significant incidents. Where the criminal nature of an incident is suspected, CERT-EU shall advise on how to report the incident to law enforcement authorities.	4. By ... [one year after the date of entry into force of the Regulation], the IICB shall issue guidance on incident response coordination and cooperation for significant incidents. Where the criminal nature of an incident is suspected, IICB and CERT-EU shall advise on how to report the incident to law enforcement authorities without undue delay.	4. The IICB shall, by [12 months after the date of entry into force of this Regulation], on the basis of a proposal from CERT-EU, adopt issue guidance documents or recommendations on incident response coordination and cooperation for significant incidents. Where the criminal nature of an incident is suspected, CERT-EU shall advise on how to report the incident to law enforcement authorities.	
Article 22				
206	Article 22 Major attacks	Article 22 Major attacks incidents	Article 22 Management of major attacks incidents	
206a			-1. In order to support the coordinated management of major incidents at operational level affecting Union entities and to contribute to the regular exchange of relevant information	

			among Union entities and with Member States, the IICB shall develop a cyber crisis management plan based on activities detailed in Article 21(2), in close cooperation with CERT-EU and ENISA, and shall include, at least, the following elements:	
206b			-1a. coordination and information flow modalities among Union entities for the management of major incidents at operational level;	
206c			-1b. common standard operating procedures (SOPs);	
206d			-1c. a common taxonomy of major incident severity and crisis triggering points;	
206e				

			-1d. regular exercises;	
206f			-1e. secure communication channels to be used;	
206g			-1f. a point of contact for EU-CyCLONe, which shall share relevant information with EU-CyCLONe as inputs to shared situational awareness.	
Article 22(1)				
207	1. CERT-EU shall coordinate among Union institutions, bodies and agencies responses to major attacks. It shall maintain an inventory of technical expertise that would be needed for incident response in the event of such attacks.	1. CERT-EU shall coordinate among the Union institutions, bodies and agencies responses entities the handling of major attacks-incidents. In that respect, it shall maintain an inventory of the available technical expertise that would be needed for incident response in the event of such attacks major incidents and assist the IICB in coordinating Union entities' cyber crisis management plans for major incidents referred to in Article 7(2a).	1. CERT-EU shall coordinate among Union institutions, bodies and agencies entities responses to major attacks incidents . It shall maintain an inventory of technical expertise that would be needed for incident response in the event of such attacks major incidents.	

Article 22(2)				
208	2. The Union institutions, bodies and agencies shall contribute to the inventory of technical expertise by providing an annually updated list of experts available within their respective organisations detailing their specific technical skills.	2. The Union institutions, bodies and agencies entities shall contribute to the inventory of technical expertise by providing an annually updated list of experts available within their respective organisations detailing their specific technical skills.	2. The Union institutions, bodies and agencies entities shall contribute to the inventory of technical expertise by providing an annually updated list of experts available within their respective organisations detailing their specific technical skills.	
Article 22(3)				
209	3. With the approval of the concerned Union institutions, bodies and agencies, CERT-EU may also call on experts from the list referred to in paragraph 2 for contributing to the response to a major attack in a Member State, in line with the Joint Cyber Unit's operating procedures.	3. With the approval of the concerned Union institutions, bodies and agencies entities concerned , CERT-EU may also call on experts from the list referred to in paragraph 2 for contributing to the response to a major attack incident in a Member State, in line with the Joint Cyber Unit's operating procedures operating procedures of EU CyCLONE. Specific rules on access to and use of technical experts from Union entities shall be approved by IICB at the proposal of CERT-EU.	3. With the approval of the concerned Following a specific request from a Member State in which the affected Union institutions, bodies and agencies entity is located and with the approval of the affected Union entity , CERT-EU may also call on experts from the list referred to in paragraph 2 for contributing to the response to a major attack in a Member State, in line with the Joint Cyber Unit's operating procedures incident in that Union entity .	

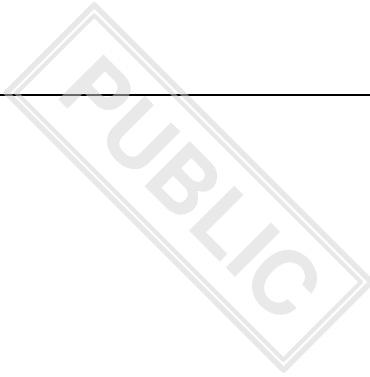


Chapter VI				
210	Chapter VI FINAL PROVISIONS	Chapter VI FINAL PROVISIONS	Chapter VI FINAL PROVISIONS	Chapter VI FINAL PROVISIONS Text Origin: Commission Proposal
Article 23				
211	Article 23 Initial budgetary reallocation	Article 23 Initial budgetary reallocation arrangements	Article 23 Initial budgetary reallocation	
211a		In its proposal for the first budget to be adopted after ... [the date of entry into force of this Regulation], the Commission shall take into account the increased budgeting and staffing needs of all Union entities, in particular those of the small Union entities, that are associated with the obligations arising from this Regulation.		

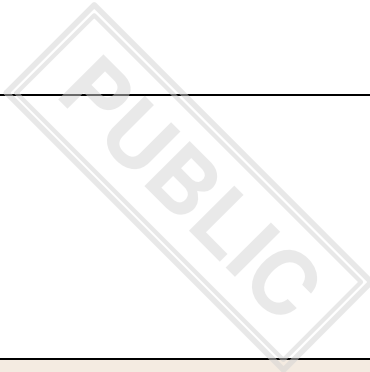
Article 23, first paragraph				
212	<p>The Commission shall propose the reallocation of staff and financial resources from relevant Union institutions, bodies and agencies to the Commission budget. The reallocation shall be effective at the same time as the first budget adopted following the entry into force of this Regulation.</p>	<p>In order to ensure proper and stable functioning of CERT-EU, the Commission shall may propose the reallocation of staff and financial resources to the Commission budget for use in CERT-EU operations from the ICT budgets of certain from relevant Union institutions, bodies and agencies to the Commission budget entities on the basis of clear criteria and without prejudice to their cybersecurity. The reallocation shall be effective at the same time as the first budget adopted following the entry into force of this Regulation-</p>	<p>The Commission shall propose the reallocation of staff and financial resources from relevant Union institutions, bodies and agencies entities to the Commission budget. The reallocation shall be effective at the same time as the first budget adopted following the entry into force of this Regulation.</p>	
Article 24				
213	Article 24 Review	Article 24 Review	Article 24 Review	<p>Article 24 Review</p> <p>Text Origin: Commission Proposal</p>

Article 24(1)				
214	1. The IICB, with the assistance of CERT-EU, shall periodically report to the Commission on the implementation of this Regulation. The IICB may also make recommendations to the Commission to propose amendments to this Regulation.	1. The IICB, with the assistance of CERT-EU shall report, at least once a year, shall periodically report to the Commission on the implementation of this Regulation. The IICB may also make recommendations to the Commission to propose amendments to this Regulation.	1. The IICB, with the assistance of CERT-EU, shall periodically report to the Commission on the implementation of this Regulation. The IICB may also make recommendations to the Commission to propose amendments to review this Regulation.	
Article 24(2)				
215	2. The Commission shall report on the implementation of this Regulation to the European Parliament and the Council at the latest 48 months after the entry into force of this Regulation and every three years thereafter.	2. The Commission shall evaluate and report on the implementation of this Regulation and on the experience gained at a strategic and operational level to the European Parliament and the Council at the latest 48 by ... [36 months after the date of entry into force of this Regulation] and every three two years thereafter.	2. The Commission shall report on the implementation of this Regulation to the European Parliament and the Council at the latest 48-36 months after the entry into force of this Regulation and every three years thereafter.	
215a		2a. The reports referred to in paragraph 2 of this Article shall evaluate, taking into account		

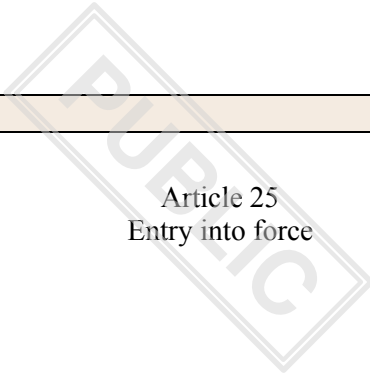
		Article 15(1a), the possibility of setting up CERT-EU as a Union office.		
Article 24(3)				
216	3. The Commission shall evaluate the functioning of this Regulation and report to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions no sooner than five years after the date of entry into force.	3. The Commission shall evaluate the functioning of this Regulation and report to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions no sooner than five years after the date of entry into force.	3. The Commission shall evaluate the functioning of this Regulation and report to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions no sooner later than five years after the date of entry into force. The report shall be accompanied, where necessary, by a legislative proposal.	
216a		Article 24a Exercise of the delegation		
216b		1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.		



216c		2. The power to adopt delegated acts referred to in Article 18(3a) shall be conferred on the Commission for an indeterminate period of time from ... [one day after the date of entry into force of this Regulation].		
216d		3. The delegation of power referred to in Article 18(3a) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.		



216e		4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.		
216f		5. A delegated act adopted pursuant to Article 18(3a) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.		



Article 25				
217	Article 25 Entry into force	Article 25 Entry into force	Article 25 Entry into force	Article 25 Entry into force Text Origin: Commission Proposal
Article 25, first paragraph				
218	This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.	This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.	This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.	This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. Text Origin: Commission Proposal
Article 25, second paragraph				
219	This Regulation shall be binding in its entirety and directly applicable in all Member States.	This Regulation shall be binding in its entirety and directly applicable in all Member States.	This Regulation shall be binding in its entirety and directly applicable in all Member States.	This Regulation shall be binding in its entirety and directly applicable in all Member States. Text Origin: Commission Proposal



Formula				
220	Done at Brussels,	Done at Brussels...	Done at Brussels,	
Formula				
221	For the European Parliament	For the European Parliament	For the European Parliament	For the European Parliament <small>Text Origin: Commission Proposal</small>
Formula				
222	The President	The President	The President	The President <small>Text Origin: Commission Proposal</small>
Formula				
223	For the Council	For the Council	For the Council	For the Council <small>Text Origin: Commission Proposal</small>
Formula				
224	The President	The President	The President	The President <small>Text Origin: Commission</small>

Annex I

225

Annex I

*deleted**deleted*

Annex I, first paragraph

226

The following domains shall be addressed in the cybersecurity baseline:

*deleted**deleted*

Annex I, point (1)

227

(1) cybersecurity policy, including objectives and priorities for security of network and information systems, in particular regarding the use of cloud computing services (within the meaning of Article 4(19) of Directive [proposal NIS 2]) and technical arrangements to enable teleworking;

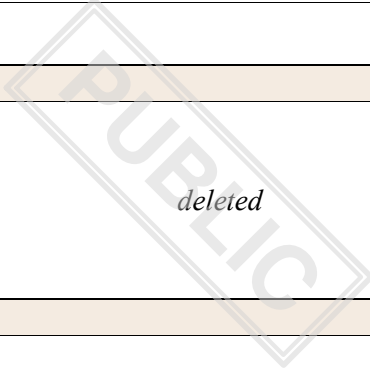
*deleted**deleted*

Annex I, point (2)

228

(2) organisation of cybersecurity, including definition of roles and responsibilities;

*deleted**deleted*



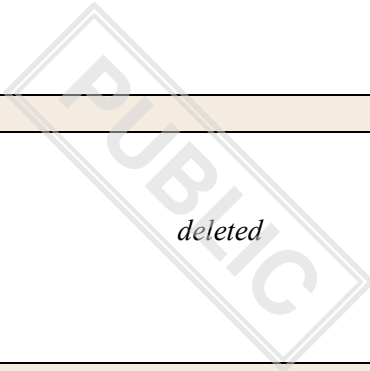
<i>Annex I, point (3)</i>				
229	(3) asset management, including IT asset inventory and IT network cartography;	<i>deleted</i>	<i>deleted</i>	
<i>Annex I, point (4)</i>				
230	(4) access control;	<i>deleted</i>	<i>deleted</i>	
<i>Annex I, point (5)</i>				
231	(5) operations security;	<i>deleted</i>	<i>deleted</i>	
<i>Annex I, point (6)</i>				
232	(6) communications security;	<i>deleted</i>	<i>deleted</i>	
<i>Annex I, point (7)</i>				
233	(7) system acquisition, development and maintenance;	<i>deleted</i>	<i>deleted</i>	
<i>Annex I, point (8)</i>				
234				

	(8) supplier relationships;	<i>deleted</i>	<i>deleted</i>	
<i>Annex I, point (9)</i>				
235	(9) incident management, including approaches to improve the preparedness, response to and recovery from incidents and cooperation with CERT-EU, such as the maintenance of security monitoring and logging;	<i>deleted</i>	<i>deleted</i>	
<i>Annex I, point (10)</i>				
236	(10) business continuity management and crisis management; and	<i>deleted</i>	<i>deleted</i>	
<i>Annex I, point (11)</i>				
237	(11) cybersecurity education, awareness-raising and training programmes.	<i>deleted</i>	<i>deleted</i>	
<i>Annex II</i>				
238	<i>Annex II</i>	<i>deleted</i>	<i>deleted</i>	
<i>Annex II, first paragraph</i>				

239	Union institutions, bodies and agencies shall address at least the following specific cybersecurity measures in the implementation of the cybersecurity baseline and in their cybersecurity plans, in line with the guidance documents and recommendations from the IICB:	<i>deleted</i>	<i>deleted</i>	
<i>Annex II, point (1)</i>				
240	(1) concrete steps for moving towards Zero Trust Architecture (meaning a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries);	<i>deleted</i>	<i>deleted</i>	
<i>Annex II, point (2)</i>				
241	(2) the adoption of multifactor authentication as a norm across network and information systems;	<i>deleted</i>	<i>deleted</i>	
<i>Annex II, point (3)</i>				
242	(3) the establishment of software			

	supply chain security through criteria for secure software development and evaluation;	<i>deleted</i>	<i>deleted</i>	
--	--	----------------	----------------	--

PUBLIC



<i>Annex II, point (4)</i>				
243	(4) the enhancement of procurement rules to facilitate a high common level of cybersecurity through:	<i>deleted</i>	<i>deleted</i>	
<i>Annex II, point (4)(a)</i>				
244	(a) the removal of contractual barriers that limit information sharing from IT service providers about incidents, vulnerabilities and cyber threats with CERT-EU;	<i>deleted</i>	<i>deleted</i>	
<i>Annex II, point (4)(b)</i>				
245	(b) the contractual obligation to report incidents, vulnerabilities and cyber threats as well as to have appropriate incidents response and monitoring in place.	<i>deleted</i>	<i>deleted</i>	