Council of the European Union

Brussels, 16 September 2022
(OR. en)

12414/22

Interinstitutional File:
2020/0365(COD)

LIMITE

PROCIV 115	**RELEX 1174**
ENV 874	**ENER 442**
JAI 1173	**HYBRID 88**
SAN 513	**TRANS 574**
COSI 222	**CYBER 297**
CHIMIE 83	**TELECOM 367**
ENFOPOL 459	**ESPACE 96**
RECH 495	**ATO 68**
CT 165	**CSC 382**
DENLEG 69	**ECOFIN 873**
COTER 221	

'I' ITEM NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee (Part 2)
No. Cion doc.:	14262/20 + ADD1
No. prev. doc.:	12041/22, 10992/22
Subject:	Proposal for a directive of the European Parliament and of the Council on the resilience of critical entities (First reading) - Confirmation of the final compromise text with a view to agreement

I. INTRODUCTION

1. On 16 December 2020, the Commission adopted the proposal for a Directive on the resilience of critical entities (the "CER Directive")[1] addressing the need to reduce the vulnerabilities of the critical entities that are essential for the functioning of the economy. The proposal aims to repeal and replace the current Directive on the identification and designation of European Critical Infrastructure (the "ECI Directive")[2].

[1] Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities. 14262/20 + ADD 1.

[2] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

2. The proposal represents the Commission's response to measures called for in the Council conclusions on Complementary efforts to enhance resilience and counter hybrid threats adopted on 10 December 2019.[3]

3. The proposal is based on Article 114 of the Treaty on the Functioning of the European Union (TFEU). It aims to enhance the resilience of critical entities that provide services essential for vital societal functions or economic activities in the internal market.

4. In the European Parliament, the committee responsible for the proposal is the Committee on Civil Liberties, Justice and Home Affairs (LIBE). The LIBE Committee adopted the Rapporteur's report on 18 October 2021 (approved in plenary on 20 October 2021).[4]

5. The European Economic and Social Committee adopted its opinion on 27 April 2021.[5]

6. In February 2021, the Permanent Representatives Committee decided to consult the European Committee of Regions on the proposal. The European Committee of the Regions gave its opinion on 1 July 2021.[6]

7. The European Data Protection Supervisor adopted its opinion on 13 August 2021.[7]

8. The Council adopted its General Approach on 20 December 2021.[8]

II. NEGOTIATIONS WITH THE EUROPEAN PARLIAMENT

9. The negotiations with Parliament and Commission started with an informal political trilogue on 31 January 2022. Another two political trilogues were held on 26 April and 28 June, supported by 42 tripartite meetings at technical level. At the political trilogue of 28 June, a political agreement was reached. At the technical meeting of 1 September, this agreement was finalised on the text set out in the Annex to this note.

10. The Presidencies negotiating the CER Directive paid special attention to the complementarity and interrelation of the CER with two related pieces of Union legislation being negotiated in parallel, namely the Directive on measures for a high common level of cybersecurity across

3 14972/19.
4 A9-0289/2021.
5 8416/21.
6 10580/21.
7 11280/21.
8 14594/21.

the Union ("the NIS2 Directive") and the proposal on the Regulation on digital operational resilience for the financial sector (the "DORA Regulation").

11. Key elements of the final compromise text are as follows:

- **The scope** (the Annex of the Directive, as well as the national security exclusion clause of Article 1.5): The scope of the agreed text of the final compromise covers 11 different sectors. A key element of the final compromise consists of a limited inclusion of the public administration sector, covering only central level administration entities and excluding the judiciary, parliaments and central banks. Furthermore, certain categories of entities in the food sector have been included in the scope of the Directive.
  In line with the Council mandate, an exclusion clause has been added to the Directive, which allows Member States to exclude specific entities that carry out their activities in the areas of defence, national security, public security or law enforcement.
- **List of essential services** (Article 4.1): The compromise text includes the setting-up, via a Delegated Act, of a non-exhaustive list of essential services in the sectors and subsectors referred to in the Annex.
- **Resilience Measures** (Article 11): In line with the Council mandate, Member States will have an appropriate level of flexibility when specifying the resilience measures that the critical entities must undertake. The Commission will adopt non-binding guidelines to further specify the technical, security and organisational measures that can be taken.
- **Cooperation among two or more Member States** (Article 9a): In line with the Council mandate, a provision has been added that foresees consultations between two or more Member States when they have critical entities that are connected in some way or when the critical entity identified in one Member State provides essential services to or in other Member States.
- **Critical entities of particular European significance** (Articles 14 and 15): A key element of the compromise was the agreement on the threshold to be identified as critical entity of particular European significance, in which Council and Parliament positions differed. The compromise found is that an entity will be considered as critical entity of particular European significance when it provides the same or similar essential services to or in six or more Member States. In line with the Council

mandate, the process of identification of such entities and the conduct of advisory missions has been further clarified.

III. CONCLUSION

12. On the basis of the above Coreper is invited to:

– approve the final compromise text, as set out in the Annex to this note, and

– confirm that the Presidency can indicate to the European Parliament that, should the European Parliament adopt its position at first reading as regards the Directive of the European Parliament and of the Council on the resilience of critical entities as set out in the Annex to this note, subject to revision of this text by the lawyer-linguists of both Institutions, the Council would approve the European Parliament's position and the act shall be adopted in the wording which corresponds to the European Parliament's position.

PE-CONS No/YY - 2020/0365 (COD)

DIRECTIVE (EU) NO …/…
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of …

on the resilience of critical entities

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[1],

Having regard to the opinion of the Committee of the Regions[2],

Acting in accordance with the ordinary legislative procedure[3],

1 OJ C , , p. .
2 OJ C […], […], p. […].
3 Position of the European Parliament […] and of the Council […].

Whereas:

(-1) Critical entities, as providers of essential services, play an indispensable role in the maintenance of vital societal functions or economic activities in the internal market, in an increasingly interdependent Union economy. It is therefore essential to set out a Union-wide framework with the aim of both enhancing the resilience of critical entities in the internal market by laying down harmonised minimum rules and assisting them through coherent, dedicated support and supervision measures.

(1) Council Directive 2008/114/EC[4] provides for a procedure for designating European critical infrastructures in the energy and transport sectors, the disruption or destruction of which would have significant cross-border impact on at least two Member States. That Directive ***focuses*** exclusively on the protection of such infrastructures. However, the evaluation of Directive 2008/114/EC conducted in 2019[5] found that due to the increasingly interconnected and cross-border nature of operations using critical infrastructure, protective measures relating to individual assets alone are insufficient to prevent all disruptions from taking place. Therefore, it is necessary to shift the approach towards ensuring ***that risks are better accounted for, that the role and duties of critical entities as providers of services essential to the functioning of the internal market are better defined and coherent, and that Union-wide rules are adopted to enhance*** the resilience of critical entities ▌***. Critical entities should be in a position to reinforce*** their ability to ***prevent, protect against, respond to, resist,*** mitigate, absorb, accommodate ▌ and recover from incidents that have the potential to disrupt the ***provision*** of ***essential services***.

4 Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p.75).

5 SWD(2019) 308.

(2) ***While a number of*** measures at Union[6] and national level ***aim to support*** the protection of critical infrastructures in the Union, ***more should be done to better equip*** the entities operating those infrastructures ▌ to address ***the*** risks to their operations that may result in ***the disruption*** of the provision of ▌ essential ***services***. This is due to a dynamic threat landscape ▌ ***, including*** evolving ***hybrid and*** terrorist ***threats,*** and growing interdependencies between infrastructures and sectors ▌ ***. Moreover, there is*** an increased physical risk due to natural disasters and climate change, which ***intensifies*** the frequency and scale of extreme weather events and brings long-term changes in average climate that can reduce the capacity ▌ ***,*** efficiency ***and lifespan*** of certain infrastructure types if ▌ climate adaptation measures are not in place. ***At the same time, the internal market is characterised by fragmentation in respect of the identification of critical entities, as*** relevant sectors and ***categories*** of entities are not recognised consistently as critical in all Member States. ***This directive therefore should achieve a solid level of harmonisation in terms of the sectors and categories of entities covered.***

[6] European Programme for Critical Infrastructure Protection (EPCIP).

(2b) ***While certain sectors of the economy, such as energy and transport, are already regulated by sector-specific acts of Union law, those acts contain provisions which relate only to certain aspects of resilience of entities operating in those sectors. In order to address in a comprehensive manner the resilience of those entities that are critical for the proper functioning of the internal market, this Directive creates an overarching framework that addresses critical entities' resilience in respect of all hazards, that is, natural and man-made, accidental and intentional.***

(3) ***The*** growing interdependencies ***between infrastructures and sectors*** are the result of an increasingly cross-border and interdependent network of service provision using key infrastructures across the Union in the sectors of energy, transport, banking, financial market infrastructure, digital infrastructure, drinking and waste water, ***food production, processing and distribution,*** health, certain aspects of public administration, as well as space ▌***. The space sector is covered with respect to*** the provision of certain services depending on ground-based infrastructures that are owned, managed and operated either by Member States or by private parties ▌, therefore not covering infrastructures owned, managed or operated by or on behalf of the Union as part of its space programmes.

In terms of the energy sector and in particular the methods of electricity generation and transmission (in respect of supply of electricity), it is understood that where deemed appropriate, electricity generation may include electricity transmission parts of nuclear power plants, but exclude the specifically nuclear elements covered by relevant nuclear legislation including treaties and Union law. The process for identifying critical entities in the food sector should adequately reflect the nature of the Union market in that sector and the extensive Union rules relating to the general principles and requirements of food law and food safety. Therefore, in order to set out a proportionate approach, and to adequately reflect the role and importance of these entities at national level, critical entities should only be identified among food businesses, whether for profit or not and whether public or private, that are engaged exclusively in logistics and wholesale distribution, and large scale industrial production and processing with a significant market share as observed at national level. These interdependencies mean that any disruption ***of essential services***, even one ***which is*** initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-***term*** negative impacts ***on*** the delivery of services across the internal market. ***Major crises such as the*** COVID-19 pandemic ***have*** shown the vulnerability of our increasingly interdependent societies in the face of ***high-impact-***low-probability risks.

(4) The entities involved in the provision of essential services are increasingly subject to diverging requirements imposed under the laws of the Member States. The fact that some Member States have less stringent security requirements on ***those*** entities not only ***creates various levels of resilience, but also*** risks impacting negatively on the maintenance of vital societal functions or economic activities across the Union, it also leads to obstacles to the proper functioning of the internal market. ***Investors and companies can rely on and trust critical entities that are resilient, reliability and trust being the cornerstones of a well-functioning internal market.*** Similar types of entities are considered as critical in some Member States but not in others, and those which are identified as critical are subject to divergent requirements in different Member States. This results in additional and unnecessary administrative burdens for companies operating across borders, notably for companies active in Member States with more stringent requirements. ***A Union framework will therefore also have the effect of levelling the playing field for critical entities across the Union.***

(5) It is therefore necessary to lay down harmonised minimum rules to ensure the provision of essential services in the internal market***, to*** enhance the resilience of critical entities ***and to improve cross-border cooperation between competent authorities. It is important that those rules be future-proof in terms of their design and implementation, allowing for the necessary flexibility. It is also crucial to improve the capacity of critical entities to provide essential services in the face of a diverse set of risks.***

(6) In order to achieve ***a high level of resilience***, Member States should identify critical entities that ***will*** be subject to specific requirements and oversight, but also particular support and guidance ▌ in the face of all relevant risks.

▌

(8) Given the importance of cybersecurity for the resilience of critical entities and in the interest of consistency, a coherent approach between this Directive and Directive (EU) XX/YY of the European Parliament and of the Council[7] [Proposed Directive on measures for a high common level of cybersecurity across the Union; (hereafter ″NIS 2 Directive″)] is necessary wherever possible. In view of the higher frequency and particular characteristics of cyber risks, the NIS 2 Directive imposes comprehensive requirements on a large set of entities to ensure their cybersecurity. Given that cybersecurity is addressed sufficiently in the NIS 2 Directive, the matters covered by it should be excluded from the scope of this Directive, without prejudice to the particular regime for entities in the digital infrastructure sector.

(9) Where provisions of other acts of Union law require critical entities to assess relevant risks, take measures to ensure their resilience or notify incidents, and ***where*** those requirements are ***recognised by Member States, pursuant to [article 1.3], as*** at least equivalent to the corresponding obligations laid down in this Directive, the relevant provisions of this Directive should not apply, so as to avoid duplication and unnecessary burdens. In that case, the relevant provisions of such other acts should apply. Where the relevant provisions of this Directive do not apply, its provisions on supervision and enforcement should not be applicable either. ▌

[7] [Reference to NIS 2 Directive, once adopted.]

(9a) This Directive should not be deemed to affect the competences of Member States and of their authorities in terms of administrative autonomy, or affect their responsibility to safeguard national security and defence or their power to safeguard other essential state functions, particularly concerning public security, territorial integrity and maintaining law and order. The exclusion of public administration entities from the scope of this Directive should apply to those entities whose activities are predominantly carried out in the areas of defence, national security, public security, or law enforcement. Public administration entities whose activities are only marginally related to such areas should still be covered by this Directive. For the purpose of this Directive, entities with regulatory competences are not considered as carrying out activities in the area of law enforcement and, therefore, are not excluded on these grounds from the scope of this Directive. Public administration entities that are jointly established with a country outside the EU in accordance with an international agreement, are not within the scope of this Directive. This Directive does not apply to Member States' diplomatic and consular missions in third countries.

Certain critical entities carry out activities in the areas of defence, national security, public security or law enforcement or provide services exclusively to the public administration entities that carry out activities predominantly in the areas of defence, national security, public security, or law enforcement. In view of the Member States' responsibility to safeguard national security and defence, Member States may decide that the obligations on critical entities pursuant to this Directive should not apply in whole or in part to those critical entities if the services they provide or the activities they perform are predominantly related to the areas of defence, national security, public security or law enforcement. Critical entities whose services or activities are only marginally related to such areas should still be covered by this Directive. No Member State should be obliged to supply information the disclosure of which would be contrary to the essential interests of its security. National or Union rules for protecting classified information and non-disclosure agreements are of relevance.

(9b) ***In order not to jeopardize the security of Member States or the security and commercial interests of critical entities, the access to, exchange and handling of sensitive information should be done prudently and with particular attention to the transmission channels and storage capacities that will be used.***

(10) In view of ensuring a comprehensive approach to the resilience of critical entities, each Member State should have ***in place*** a strategy setting out objectives and policy measures to be implemented. ***In the interest of coherence and efficiency, that strategy should be designed to seamlessly integrate existing policies, building wherever possible upon relevant existing national and sectoral strategies, plans or similar documents.*** To achieve ***a comprehensive approach***, Member States should ensure that their ▌ strategies provide for a policy framework for enhanced coordination between the competent authority under this Directive and ***under*** the NIS 2 Directive in the context of information sharing on ***cybersecurity risks, cyber threats and*** incidents and ***non-***cyber ***risks,*** threats and ***incidents and of*** the exercise of supervisory tasks. ***When putting in place those strategies, Member States should take due account of the hybrid nature of threats to critical entities.***

(10a) Member States should communicate their strategy on the resilience of critical entities and substantial updates thereof to the Commission, in particular to enable the Commission to assess the correct application of this Directive as regards policy approaches to critical entities' resilience at national level. The strategies could be communicated as classified information, if needed. The Commission should draw up a summary report of the strategies communicated by Member States to serve as a basis for exchanges to identify best practices and issues of common interest in the framework of the Critical Entities Resilience Group. Due to the sensitive nature of the aggregated information which will be contained in the summary report - whether classified or not - the Commission should manage this summary report with appropriate level of awareness with respect to the security of the critical entities, Member States and the European Union. The summary report and the strategies of Member States should be safeguarded against unlawful or malicious action and should be accessible only to authorized persons in order to fulfil the objectives of this Directive. The communication of the strategies and substantial updates thereof should also help to understand developments in approaches to critical entities' resilience and feed into the monitoring of the impact and added value of this Directive, which the Commission is to review periodically.

(11) The actions of Member States to identify and help ensure the resilience of critical entities should follow a risk-based approach that targets efforts to the entities most relevant for the performance of vital societal functions or economic activities. In order to ensure such a targeted approach, each Member State should carry out, within a harmonised framework, an assessment of ***the*** relevant natural and man-made risks***, including those of a cross-sectoral or cross-border nature,*** that may affect the provision of essential services, including accidents, natural disasters, public health emergencies such as pandemics, ***hybrid threats or other*** antagonistic threats, including terrorist offences***, criminal infiltration and sabotage***. When carrying out those risk assessments, Member States should take into account other general or sector-specific risk assessment carried out pursuant to other acts of Union law and should consider the dependencies between sectors, including from other Member States and third countries. The outcomes of the risk assessment should be used in the process of identification of critical entities and to assist those entities in meeting ***their*** resilience requirements ▌***. This*** Directive ***applies only to Member States and critical entities that operate within the Union.***

Nonetheless, the expertise and knowledge generated by Member States' competent authorities, notably through risk assessments, as well as by the Commission, notably through various forms of support and cooperation, could be used, where appropriate and in accordance with the applicable legal instruments, for the benefit of third countries, notably those in the direct neighbourhood of the Union, by feeding into existing cooperation on resilience.

(12) In order to ensure that all relevant entities are subject to ***the resilience*** requirements ***of this Directive*** and to reduce divergences in this respect, it is important to lay down harmonised rules allowing for a consistent identification of critical entities across the Union, while also allowing Member States to ***adequately*** reflect ***the role and importance of these entities at*** national ***level. Applying the*** criteria ***laid down in this Directive, Member States should*** identify ▌ entities ***that provide one or more essential services and that operate and have critical infrastructure located on the territory of that Member State. An entity should be considered to operate on the territory of the Member State where it carries out activities necessary for the essential service or services in question, and where that entity's critical infrastructure, which is used to provide that service or those services, is located. If there is no entity meeting those criteria in a Member State, that Member State should have no obligation to identify a critical entity in the corresponding sector or sub-sector***. In the interest of effectiveness, efficiency, consistency and legal certainty, appropriate rules should also be set on notification ▌ of ▌ such identification. ▌

(12a) Member States should submit to the Commission, in a manner that ***serves the objectives of this Directive***, the list of essential services, the number of critical entities identified for each sector and subsector referred to in the Annex and ***for*** the essential service or services that each entity provides and***, if applied,*** thresholds***, which could be presented as such or in aggregated form, meaning that the information can be averaged by geographic area, by year, sector, sub-sector, or by other means, and can include information on the range of the indicators provided***.

(13) Criteria should also be established to determine the significance of a disruptive effect produced by such incidents. Those criteria should build on the criteria provided in Directive (EU) 2016/1148 of the European Parliament and of the Council[8] in order to capitalise on the efforts carried out by Member States to identify those operators and the experience gained in this regard. ***Major crises such as the COVID-19 pandemic have shown the importance of ensuring the supply chain security and demonstrated how its disruption can have negative economic and societal impacts across a large number of sectors and across borders. Therefore, Member States should also consider effects on the supply chain, to the extent possible, when determining the dependency of other sectors and subsectors.***

[8] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

(13c) In accordance with applicable Union and national law, including Regulation (EU) 2019/452 of the European Parliament and of the Council[9], which establishes a framework for the screening of foreign direct investments in the Union, the potential threat posed by foreign ownership of critical infrastructure within the Union is to be acknowledged because services, the economy and the free movement and safety of Union citizens depend on the proper functioning of critical infrastructure.

(14) ***Directive XXXX/XXXX [NIS2 Directive] requires entities in*** the digital infrastructure sector***, which may qualify as critical entities under this Directive, to take appropriate technical, operational and organisational measures to manage the risks posed to the security of*** network and information systems ***as well as to notify significant incidents and cyber threats. Since threats to*** the ***security*** of ***network and information systems can have different origins,*** the ***[***NIS 2 Directive ▌ ***] applies an "all-hazard" approach that includes the resilience of network and information*** systems***, as well as*** their ***physical components and environments.***

---

9 ***Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union (OJ L 79I, 21.3.2019, p. 1).***

Given that those ***requirements*** are ***at least equivalent to the corresponding*** obligations ***laid down in*** this Directive***, Article 9a and Chapters III, IV and VI should*** not apply to ***those*** entities***, to avoid duplication and unnecessary administrative burden***. However, considering the importance of the services provided by entities in the digital infrastructure sector ***to critical entities belonging to all*** other ***sectors***, Member States should identify, based on the criteria and using the procedure provided for in this Directive mutatis mutandis, entities ▌ to the digital infrastructure sector ▌ as ▌ critical entities ▌. ***Consequently, the dedicated strategies for reinforcing the resilience of*** critical entities***, the risk assessments and the support measures as set out*** in Chapter II ***of this Directive*** should ▌ be ***applicable. Member States may adopt or maintain provisions of national law to achieve a higher level of resilience for those critical entities provided that those national provisions are consistent with applicable Union law***.

(15) The EU financial services acquis establishes comprehensive requirements on financial entities to manage all risks they face, including operational risks and ensure business continuity. This includes Regulation (EU) No 648/2012 of the European Parliament and of the Council[10], Directive 2014/65/EU of the European Parliament and of the Council[11] and Regulation (EU) No 600/2014 of the European Parliament and of the Council[12] as well as Regulation (EU) No 575/2013 of the European Parliament and of the Council[13] and Directive 2013/36/EU of the European Parliament and of the Council[14]. The ***legal*** framework ***is complemented*** with Regulation XX/YYYY of the European Parliament and of the Council [proposed Regulation on digital operational resilience for the financial sector (hereafter ***"***DORA Regulation***"***)[15]], which lays down requirements for financial firms to manage ICT risks, including the protection of physical ICT infrastructures. Since the resilience of entities ▌ is ***therefore*** comprehensively covered***, Article 9a and Chapters III, IV and VI of this Directive should not apply to those entities, to avoid duplication and unnecessary administrative burden.***

10 Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).

11 Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

12 Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 (OJ L 173, 12.6.2014, p. 84).

13 Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

14 Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

15 Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, COM(2020) 595.

However, considering the importance of the services provided by ***entities in*** the ▌financial ***sectors to critical entities belonging to all other sectors, Member States should identify, based on the criteria and using the procedure provided for in this Directive mutatis mutandis, entities in the financial sectors*** as ▌critical entities ▌***. Consequently,*** the ***dedicated strategies for reinforcing the resilience of critical entities, the risk assessments and the support measures as set out in*** Chapter II of this Directive ***should be applicable. Member States may adopt or maintain provisions of national law to achieve a higher level of*** resilience ***for those*** critical entities ***provided that those national provisions are consistent with applicable Union law***.

(16) Member States should designate authorities competent to supervise the application of and, where necessary, enforce the rules of this Directive and ensure that those authorities are adequately empowered and resourced. In view of the differences in national governance structures and in order to safeguard already existing sectoral arrangements or Union supervisory and regulatory bodies, and to avoid duplication, Member States should be able to designate more than one competent authority. In that case, they should however clearly delineate the respective tasks of the authorities concerned and ensure that they cooperate smoothly and effectively. All competent authorities should also cooperate more generally with other relevant authorities, both at national and Union level.

(17) In order to facilitate cross-border cooperation and communication and to enable the effective implementation of this Directive, each Member State should, without prejudice to sector-specific Union legal requirements, designate ***one national single point of contact, where relevant within a*** competent authority ▌***,*** responsible for coordinating issues related to the resilience of critical entities and cross-border cooperation at Union level in this regard. ***Each single point of contact should liaise and coordinate communication, where relevant, with the competent authorities of its Member State, with the single points of contact of other Member States and with the Critical Entities Resilience Group.***

(18) ▌***The*** competent authorities designated under ***this Directive and those designated under [NIS 2 Directive]*** should cooperate ***and exchange information***, in relation to cybersecurity risks***, cyber threats and incidents and non-cyber risks, threats*** and incidents affecting ***critical*** entities ***as well as on relevant measures taken by competent authorities designated under [the NIS 2 Directive] and this Directive. It is important that Member States ensure that requirements provided for in this Directive and [the NIS 2 Directive] are implemented in a complementary way and that critical entities are not subject to an administrative burden beyond that which is necessary to achieve the objectives of these Directives***.

(19) Member States should support critical entities***, including those that qualify as small or medium-sized enterprises (SMEs),*** in strengthening their resilience, in compliance with their obligations under this Directive, without prejudice to the entities' own legal responsibility to ensure such compliance ***and in doing so, prevent excessive administrative burdens***. Member States could in particular develop guidance materials and methodologies, support the organisation of exercises to test their resilience and provide ***advice and*** training to personnel of critical entities. ***Where necessary and justified by public interest objectives, Member States could provide financial resources and should facilitate*** voluntary information sharing ***and good practices exchange*** between critical entities, without prejudice to the application of competition rules laid down in the Treaty on the Functioning of the European Union.

(19a) With the aim of enhancing the resilience of critical entities identified by Member States and in order to reduce the administrative burden for those entities, the designated competent authorities of Member States should engage in consultations whenever appropriate for the consistent application of this Directive. Those consultations should be entered into at the request of any interested competent authority, and should focus on ensuring a convergent approach regarding inter-linked critical entities that use critical infrastructure which is physically connected between two or more Member States, that belong to the same groups or corporate structures, or that have been identified in one Member State and provide essential services to or in other Member States.

(19c) Where provisions of Union or national law require critical entities to assess risks relevant for the purposes of this Directive and to take measures to ensure their own resilience, those requirements should be adequately considered for the purposes of supervising critical entities' compliance with this Directive.

(20) ***Critical*** entities should have a comprehensive understanding of ***the*** relevant risks to which they are exposed and ***a duty to*** analyse those risks. To that ***effect***, they should carry out risks assessments, whenever necessary in view of their particular circumstances and the evolution of those risks, ***and*** in any event every four years. ***Where*** critical entities ***have undertaken assessments of risk or drawn up documents pursuant to obligations in other acts of law that are relevant for the risk assessment pursuant to this Directive, they may use those assessments and documents to meet the requirements set out in this Directive. With the same aim, a competent authority may declare an existing risk assessment of a critical entity that addresses those risks and dependencies as compliant with the requirements of this Directive in whole or in part***.

(21) Critical entities should take organisational***, security*** and technical measures that are appropriate and proportionate to the risks they face so as to prevent***, protect against, respond to***, resist, mitigate, absorb, accommodate and recover from an incident. ***While*** critical entities should take measures ***in accordance with Article [11]***, the details and extent of the measures should reflect the different risks that each entity has identified as part of its risk assessment and the specificities of such entity in an appropriate and proportionate way. ***To promote a coherent Union-wide approach, the Commission should, after consultation of the Critical Entities Resilience Group, adopt non-binding guidelines to further specify those technical, security and organisational measures. In the performance of its duties under this Directive, each critical entity should designate a liaison officer or equivalent as point of contact with the national competent authorities.***

(22) In the interest of effectiveness and accountability, critical entities should describe ***the*** measures ***they take***, with a level of detail ***that*** sufficiently ***achieves*** those aims, having regard to the risks identified, in a resilience plan or in a document or documents that are equivalent to a resilience plan, and apply that plan in practice. ***If critical entities have already taken technical, security and organisational measures and drawn up documents pursuant to other acts of law that are relevant for resilience-enhancing measures under this Directive, they may use those measures and documents to meet their obligations to avoid unnecessary duplications. With the same aim, a competent authority may declare existing resilience measures of a critical entity that address those obligations as compliant*** with ***the*** requirements ***of this Directive in whole or in part***.

(23) Regulation (EC) No 300/2008 of the European Parliament and of the Council[16], Regulation (EC) No 725/2004 of the European Parliament and of the Council[17] and Directive 2005/65/EC of the European Parliament and of the Council[18] establish requirements applicable to entities in the aviation and maritime transport sectors to prevent incidents caused by unlawful acts and to resist and mitigate the consequences of such incidents. While the measures required in this Directive are broader in terms of risks addressed and types of measures to be taken, critical entities in those sectors should reflect in their resilience plan or equivalent documents the measures taken pursuant to those other Union acts. Moreover, ***critical entities are also to take into consideration Directive 2008/96/EC of the European Parliament and of the Council[19], which introduces a network-wide road assessment to map the risks of accidents and a targeted road safety inspection to identify hazardous conditions, defects and problems that increase the risk of accidents and injuries, based on a site visit of an existing road or section of road.***

16 Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97/72, 9.4.2008, p. 72).

17 Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p. 6.).

18 Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28).

19 Directive 2008/96/EC of the European Parliament and of the Council of 19 November 2008 on road infrastructure safety management (OJ L 319, 29.11.2008, p. 59).

Ensuring the protection and resilience of critical entities is of the utmost importance for the railway sector and, when implementing resilience measures under this Directive, critical entities ***are encouraged to refer*** to non-binding guidelines and good practices documents developed under sectorial workstreams, such as the EU Rail Passenger Security Platform[20].

(24) The risk of employees of critical entities ***or contractors*** misusing for instance their access rights within the entity's organisation to harm and cause damage is of increasing concern. ***Member States should*** therefore ***specify the conditions according*** to ***which*** critical entities ***are permitted, in duly reasoned cases and taking into account the risk assessments at national level, to submit requests for*** background checks on persons falling within specific categories of its personnel ▌***. It should be ensured*** that ▌ requests are assessed ***within a reasonable timeframe*** by the relevant authorities ***and processed*** in accordance with ***national legislation and procedures, as well as relevant and*** applicable ▌ Union ▌ law, including on the protection of personal data. ***In order to corroborate the identity of a person that is subject to a background check, it is appropriate for Member States to require a proof of identity, such as a passport, national identity card or digital forms of identification, in accordance with applicable law.***

[20] Commission Decision of 29 June 2018 setting up the EU Rail Passenger Security Platform C/2018/4014.

Such background check should also include criminal records and for that purpose draw on information obtained from the European Criminal Records Information System (ECRIS) in accordance with the procedures set out in Council Framework Decision 2009/315/JHA, and, where relevant and applicable, Regulation (EU) 2019/816 of the European Parliament and of the Council[21]. Member States might also, where relevant and applicable, draw on the Second Generation Schengen Information System (SIS II)[22], intelligence as well as any other objective information available that might be necessary to determine the suitability of the person concerned to work in the position in relation to which the critical entity has requested a background check.

---

21 ***Council Framework Decision 2009/315/JHA and Regulation (EU) 2019/816 of the European Parliament and of the Council of 22 May 2019, OJ L 135, p. 1.***

22 ***Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, OJ L 312, p. 56.***

(25) ***A mechanism for the notification of certain incidents should be established to allow the competent authorities to respond to the incidents rapidly and adequately and to have a comprehensive overview of impacts, nature, cause and possible consequences of an incident which the critical entities deal with. Critical entities should notify without undue delay Member States' competent authorities of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services. Unless operationally unable to do so, critical entities should send an initial notification no later than 24 hours after becoming aware of the incident. The initial notification should only include the information strictly necessary to make the competent authority aware of the incident and allow the entity to seek assistance, if required. Such notification should indicate, where possible, the presumed cause of an incident. Member States should ensure that the requirement to submit this initial notification does not divert the reporting entity's resources from activities related to incident handling that should be prioritised. The initial notification should be followed, where relevant, by a detailed report no later than one month after the incident. The detailed report should complement the initial notification and provide a more complete overview of the incident***.

(26) While critical entities generally operate as part of an increasingly interconnected network of service provision and infrastructures and often provide essential services in more than one Member State, some of those entities are of particular significance for the Union ***and its internal market*** because they provide essential services to ***or in six*** Member States ***or more of*** and therefore ***could benefit from*** specific ***support*** at Union level. Rules on ***advisory missions*** in respect of such critical entities of particular European significance should therefore be established. Those rules are without prejudice to the rules on supervision and enforcement set out in this Directive.

(27) ***Upon the reasoned request of one or more Member States to or in which the essential service is provided or the Commission, where*** additional information is necessary to be able to advise a critical entity in meeting its obligations under ***this Directive*** or to assess the compliance of a critical entity of particular European significance with those obligations, ***the Member State that has identified a critical entity of particular European significance as critical entity shall provide the Commission with certain information. In*** agreement with the Member State ***that identified*** the ***critical entity of European significance as critical*** entity ▌, the Commission should ***be able to*** organise an advisory mission to assess the measures put in place by that entity. In order to ensure that such advisory missions are carried out properly, complementary rules should be established, notably on their organisation and conduct, the follow-up to be given and the obligations for the critical entities of particular European significance concerned.

The advisory missions should, without prejudice to the need for the Member State where the advisory mission is conducted and the entity concerned to comply with the rules of this Directive, be conducted subject to the detailed rules of the law of that Member State, for instance on the precise conditions to be fulfilled to obtain access to relevant premises or documents and on judicial redress. Specific expertise required for such missions could, where relevant, be requested through the Emergency Response Coordination Centre.

(27a) Standardisation should remain primarily a market-driven process. However, there might still be situations where it is appropriate to require compliance with specified standards. Member States should, where useful, encourage the use of European and internationally recognised standards and specifications relevant to resilience measures applicable to critical entities.

(28) In order to support the Commission and facilitate ▌ cooperation ***among Member States*** and the exchange of information, including best practices, on issues relating to this Directive, a Critical Entities Resilience Group ***as*** a Commission expert group, should be established. Member States should endeavour to ensure effective and efficient cooperation of the designated representatives of their competent authorities in the Critical Entities Resilience Group***, including by designating representatives holding security clearance, where appropriate***. The group should begin to perform its tasks from six months after the entry into force of this Directive, so as to provide additional means for appropriate cooperation during the transposition period of this Directive. ***The group should interact with relevant other sector specific expert working groups.***

(28a) The Critical Entities Resilience Group should cooperate with the Cooperation Group established under the [NIS 2 Directive] with a view to supporting a comprehensive framework for non-cyber and cyber resilience of critical entities. The Critical Entities Resilience Group and the Cooperation Group established under the [NIS 2 Directive] should engage in a regular dialogue to promote cooperation between the competent authorities designated under this Directive and the [NIS 2 Directive] and to facilitate the exchange of information notably on topics of relevance to both groups.

(29) In order to achieve the objectives of this Directive, and without prejudice to the legal responsibility of Member States and critical entities to ensure compliance with their respective obligations set out therein, the Commission should, where it considers it appropriate, undertake certain supporting activities aimed at facilitating compliance with those obligations. When providing support to Member States and critical entities in the implementation of obligations under this Directive, the Commission should build on existing structures and tools, such as those under the Union Civil Protection mechanism and the European Reference Network for Critical Infrastructure Protection. ***In addition, it should inform Member States about resources available at EU-level, such as within the Internal Security Fund, Horizon Europe or other instruments relevant for the resilience of critical entities.***

(30) Member States should ensure that their competent authorities have certain specific powers for the proper application and enforcement of this Directive in relation to critical entities, where those entities fall under their jurisdiction as specified in this Directive. Those powers should include, notably, the power to conduct inspections, supervision and audits, require critical entities to provide information and evidence relating to the measures they have taken to comply with their obligations and, where necessary, issue orders to remedy identified infringements. When issuing such orders, Member States should not require measures which go beyond what is necessary and proportionate to ensure compliance of the critical entity concerned, taking account of in particular the seriousness of the infringement and the economic capacity of the critical entity. More generally, those powers should be accompanied by appropriate and effective safeguards to be specified in national law, in accordance with the requirements resulting from Charter of Fundamental Rights of the European Union. When assessing the compliance of a critical entity with its obligations under this Directive, competent authorities designated under this Directive should be able to request the competent authorities designated under ***[***the NIS 2 Directive ▌***] to exercise their supervisory and enforcement powers in relation to an entity under*** the ***scope*** of ***[NIS 2 Directive] that is also identified as critical under this Directive***. Those competent authorities should cooperate and exchange information for that purpose.

(31) In order to ***apply this Directive in an effective and consistent manner***, the power to adopt acts in accordance with Article 290 ***of the*** Treaty on the Functioning of the European Union should be delegated to the Commission to supplement ***this Directive by drawing up a list of essential services. That list should be used by Member States' competent authorities for the purpose of conducting risk assessments pursuant to Article 4 and for the identification of critical entities pursuant to Article 5. In light of the minimum harmonisation approach of this Directive, this list is non-exhaustive and Member States could complement it with additional essential services at national level in order to take into account national specificities in the provision of essential services***. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[23]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

[23] OJ L 123, 12.5.2016, p. 1.

(32) In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[24].

(33) Since the objectives of this Directive, namely to ensure the provision in the internal market of services essential for the maintenance of vital societal functions or economic activities and to enhance the resilience of critical entities providing such services, cannot be sufficiently achieved by the Member States, but can rather, by reason of the effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on the European Union. In accordance with the principle of proportionality as set out in that Article 5, this Directive does not go beyond what is necessary in order to achieve those objectives.

(33a) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered an opinion on 11 August 2021 [*].

(34) Directive 2008/114/EC should therefore be repealed,

HAVE ADOPTED THIS DIRECTIVE:

---

[24] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

* ***[OJ C 20, 21.1.2019, p. 1./…]].***

Chapter I

Subject matter , Scope and Definitions

Article 1

Subject matter and scope

1. This Directive:

(a) lays down obligations for Member States to take ***specific*** measures aimed at ensuring the ***unobstructed*** provision in the internal market of services essential for the maintenance of vital societal functions or economic activities ***within the scope of Article 114 TFEU***, in particular to identify critical entities and ▌ to ***support*** them to meet their obligations;

(b) establishes obligations for critical entities aimed at enhancing their resilience and ▌ ability to provide those services in the internal market;

(c) establishes rules on supervision ▌ of critical entities ***and enforcement;***

(ca) establishes rules for the identification of critical entities ▌ of particular European significance ***and advisory missions thereto;***

(cb) establishes common procedures for cooperation and reporting for the application of the provisions of this Directive;

(cc) lays down measures with a view to achieving a high level of resilience of critical entities in order to ensure the provision of essential services within the Union and to improve the functioning of the internal market.

2. This Directive shall not apply to matters covered by Directive (EU) XX/YY [proposed Directive on measures for a high common level of cybersecurity across the Union; ('NIS 2 Directive')], without prejudice to Article 7***. In view of the relationship between cybersecurity and the physical security of critical entities, Member states shall ensure a coordinated implementation of this Directive and the NIS 2 Directive***.

3. Where provisions of sector-specific acts of Union law require critical entities to take measures ***to enhance their resilience***, and where those requirements are ***recognised by***

Member States as at least equivalent to the obligations laid down in this Directive, the relevant provisions of this Directive shall not apply, including the provisions on supervision and enforcement laid down in Chapter VI.

4. Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and ▌ the security and commercial interests of critical entities***, while respecting the security of Member States***.

4a. This Directive is without prejudice to the Member States' responsibility to safeguard national security and defence or their power to safeguard other essential state functions, including ensuring the territorial integrity of the State and maintaining law and order.

(a) This Directive does not apply to public administration entities that carry out their activities in the areas of defence, national security, public security or law enforcement, including the investigation, detection and prosecution of criminal offences.

(c) Member States may decide that for specific critical entities which carry out activities in the areas of defence, national security, public security or law enforcement, including activities relating to the investigation, detection and prosecution of criminal offences, or which provide services exclusively to the public administration entities referred to in point a, the provisions laid down in Article 9a and in Chapters III to VI, in whole or in part, shall not apply.

4b. The obligations laid down in this Directive do not entail the supply of information, the disclosure of which is contrary to the Member States' essential interests of national security, public security or defence.

4c. This Directive is without prejudice to Union law on the protection of personal data, in particular Regulation (EU) 2016/679[25] and Directive 2002/58/EC[26].

---

25 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; OJ L 119, 4.5.2016, p. 1.

26 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector; OJ L 201, 31.7.2002, p. 37.

Article 2

Definitions

For the purposes of this Directive, the following definitions apply:

(1) "critical entity" means a public or private entity ***that*** has been identified ▌ by a Member State in accordance with Article 5 ***as belonging to one of the categories referred to in the third column of the table in the Annex***;

(2) ***"***resilience***"*** means ***a critical entity's*** ability to prevent***, protect against, respond to***, resist, mitigate, absorb, accommodate ▌ and recover from an incident ▌ ;

(3) ***"***incident***"*** means any event having the potential to ***significantly*** disrupt, or that disrupts, the ***provision*** of ***an essential service, including when it affects the national systems that safeguard the rule of law;***

(4) ***"critical*** infrastructure***"*** means an asset, ***a facility, equipment, a network, a*** system or part thereof, which is necessary for the ***provision*** of an essential service;

(5) ***"***essential service***"*** means a service which is ***crucial*** for the maintenance of vital societal functions ▌ **,** economic activities***, public health and safety or the environment***;

(6) "risk" means ***the potential for loss or disruption caused by an incident and shall be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of said incident***;

(7) "risk assessment ***"*** means ***the overall process*** to determine the nature and extent of a risk by ***identifying and*** analysing potential ***relevant*** threats***, vulnerabilities*** and hazards ***that could lead to an incident*** and evaluating ***the potential loss or disruption of the provision of an essential service caused by the incident***.

(7a) 'standard' means standard as defined in Article 2, point (1), of Regulation (EU) No 1025/2012 of the European Parliament and of the Council[27];

(7b) 'technical specification' means technical specification as defined in Article 2 point (4), of Regulation (EU) No 1025/2012;

(7c) 'public administration entity' means an entity recognised as such in a Member State in accordance with national law, that complies with the following criteria:

a) it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character;

b) it has legal personality or it is entitled by law to act on behalf of another entity with legal personality;

c) it is financed, for the most part, by the State or by other central-level bodies governed by public law; or it is subject to management supervision by those authorities or bodies; or it has an administrative, managerial or supervisory board, more than half of whose members are appointed by the State or by other central-level bodies governed by public law;

---

[27] 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).

d) it has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital.

Article 2a

Minimum harmonisation

Without prejudice to their obligations under Union law, Member States may adopt or maintain provisions of national law with a view to achieving a higher level of resilience of critical entities.

Chapter II

National Frameworks on the Resilience of Critical Entities

Article 3

Strategy on the resilience of critical entities

1. ***Following a consultation that is, to the extent practically possible, open to relevant stakeholders, each*** Member State shall adopt by [three years after entry into force of this Directive] a strategy for ***enhancing*** the resilience of critical entities. This strategy shall set out strategic objectives and policy measures***, building upon relevant existing national and sectoral strategies or documents,*** with a view to achieving and maintaining a high level of resilience on the part of those critical entities and covering at least the sectors referred to in the Annex.

2. The strategy shall contain at least the following elements:

   (a) strategic objectives and priorities for the purposes of enhancing the overall resilience of critical entities taking into account cross-border and cross-sectoral ***dependencies and*** interdependencies;

   (b) a governance framework to achieve the strategic objectives and priorities, including a description of the roles and responsibilities of the different authorities, critical entities and other parties involved in the implementation of the strategy;

(c) a description of measures necessary to enhance the overall resilience of critical entities, including a ***description of the*** national risk assessment ***as referred to in Article 4;***

(ca) a description of the process by which critical entities are identified;

(cb) a description of the process supporting critical entities in accordance with this Chapter, including measures to enhance cooperation between the public sector, on the one hand, and the private sector and public and private entities on the other hand;

(cc) a list of the main authorities and relevant stakeholders, other than critical entities, involved in the implementation of the strategy;

(d) a policy framework for ▌ coordination between the competent authorities designated pursuant to Article 8 of this Directive and pursuant to [the NIS 2 Directive] for the purposes of information sharing on ***cybersecurity risks, cyber threats and*** incidents and ***non-***cyber ***risks,*** threats ***and incidents*** and the exercise of supervisory tasks***;***

(da) a description of measures already in place aimed to facilitate the implementation of obligations pursuant to chapter III by small and medium-sized enterprises within the meaning of the Annex to Commission Recommendation 2003/361/EC[28] that Member States identified as critical entities.

Following a consultation that is, to the extent practically possible, open to relevant stakeholders, the strategy shall be updated ▌ at least every four years.

3. Member States shall communicate their strategies, and ***substantial*** updates of their strategies, to the Commission within three months from their adoption.

Article 4

Risk assessment by Member States

[28] [Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).]

1. ***The Commission shall be empowered to adopt a delegated act by [10 months from the date of entry into force of this Directive], in accordance with Article 21 to supplement this Directive by establishing a non-exhaustive*** list of essential services in the sectors ***and subsectors*** referred to in the Annex. ***Competent authorities designated pursuant to Article 8 shall use this list of essential services for the purpose of carrying*** out ***a risk assessment*** by [three years after entry into force of this Directive], and subsequently where necessary, and at least every four years ▌***. Competent authorities shall use this risk*** assessment ***for*** identifying critical entities in accordance with Article ***5*** and assisting those critical entities to take measures pursuant to Article 11.

The risk assessment shall account for ***the*** relevant natural and man-made risks, including ***those of a cross-sectoral or cross-border nature,*** accidents, natural disasters, public health emergencies, ***hybrid threats or other*** antagonistic threats, including terrorist offences pursuant to Directive (EU) 2017/541 of the European Parliament and of the Council[29].

2. In carrying out the risk assessment, Member States shall take into account ***at least the following***:

(a) the general risk assessment carried out pursuant to Article 6(1) of Decision No 1313/2013/EU of the European Parliament and of the Council[30];

(b) other relevant risk assessments, carried out in accordance with the requirements of the relevant sector-specific acts of Union law, including Regulation (EU) 2019/941 of the European Parliament and of the Council[31] ▌**,** Regulation (EU) 2017/1938 ***of the European Parliament and of the Council[32], Directive 2012/18/EU of the European Parliament and of the Council[33] and Directive 2007/60/EC*** of the European Parliament and of the Council[34];

(c) ***The relevant*** risks arising from the dependencies between the sectors referred to in the Annex, including from ***dependencies on entities located within*** other Member States and third countries, and the impact that a ***significant*** disruption in one sector may have on other sectors***, including any significant risks to citizens and the internal market***;

---

29 Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, p. 6).

30 Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924).

31 Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC (OJ L 158, 14.6.2019, p. 1).

32 Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010 (OJ L 280, 28.10.2017, p. 1).

33 Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC (OJ L 197, 24.7.2012, p. 1).

34 Directive 2007/60/EC of the European Parliament and of the Council of 23 October 2007 on the assessment and management of flood risks (OJ L 288, 6.11.2007, p. 27).

(d) any information on incidents notified in accordance with Article 13.

For the purposes of point (c) of the first subparagraph, Member States shall cooperate with the competent authorities of other Member States and third countries, as appropriate.

3. Member States shall make the relevant elements of the risk assessment referred to in paragraph 1 available***, where relevant through their single points of contact,*** to the critical entities that they identified in accordance with Article 5 ▌***. The information provided*** to ▌ critical entities ***shall assist them*** in carrying out their risk assessment, pursuant to Article 10, and in taking measures to ensure their resilience pursuant to Article 11.

4. Each Member State shall provide the Commission with ***relevant information*** on the types of risks identified and the outcomes of the risk assessments, per sector and sub-sector referred to in the Annex, ***within 3 months*** after ***carrying out the risk assessment*** and subsequently where necessary and at least every four years.

5. The Commission ***shall***, in cooperation with the Member States, develop a voluntary common reporting template for the purposes of complying with paragraph 4.

Article 5

Identification of critical entities

1. By [***3*** years and ***6*** months after entry into force of this Directive] Member States shall identify ***the critical entities*** for ***the sectors*** and ***subsectors*** referred to in the Annex ▌.

2. When identifying critical entities pursuant to paragraph 1, Member States shall take into account the outcomes of the risk assessment pursuant to Article 4 and ***the strategy on the resilience of critical entities referred to in Article 3 and shall*** apply ***all*** following criteria:

(a) the entity provides one or more essential services;

(b) ***The entity operates on*** the ***territory*** of ***the Member State performing the identification and its critical*** infrastructure ***is*** located ***on*** the ***territory of this*** Member State; and

(c) ***An*** incident would have significant disruptive effects***, as determined in accordance with Article 6(1),*** on the provision of ***one*** or ***more*** of ***these*** essential services in the sectors referred to in the Annex that depend on the service.

3. Each Member State shall establish a list of the critical entities identified and ensure that those critical entities are notified of their identification as critical entities within one month of that identification ▌. ***Member States shall inform those critical entities*** of their obligations pursuant to Chapters ***III*** and ***IV*** and the date from which ***these*** provisions ▌ apply to them***, without prejudice to Article 7. Member States shall inform critical entities in the sectors referred to in points 3, 4 and 8 of the Annex that they have no obligations pursuant to Chapters III and IV, unless national provisions provide otherwise***.

For the critical entities concerned, ▌ the provisions of Chapter III shall apply from ***10*** months after ***the*** date ***of the notification referred to in the first sentence***.

4. Member States shall ensure that their competent authorities designated pursuant to Article 8 of this Directive notify the competent authorities ▌ designated in accordance with Article ***[X]*** of [the NIS 2 Directive], of the identity of the critical entities that they identified under this Article within one month of that identification.

That notification ***shall specify, where applicable,*** that ***the*** critical entities ***concerned are entities in the sectors referred to in points 3, 4 and*** 8 of ***the Annex to*** this Directive ***and*** have ***no*** obligations ***under Chapters III and IV thereof***.

▌

7. Member States shall, where necessary and in any event at least every four years, review and, where appropriate, update the list of identified critical entities.

Where those updates lead to the identification of additional critical entities, paragraphs 3 ▌ and ***4*** shall apply. In addition, Member States shall ensure that entities that are no longer identified as critical entities pursuant to any such update are notified thereof and are informed ***in due time*** that they are no longer subject to the obligations pursuant to Chapter III as from the reception of that information.

7a. The Commission shall, in cooperation with the Member States, develop recommendations and nonbinding guidelines to support Member States in identifying critical entities.

Article 6

Significant disruptive effect

1. When determining the significance of a disruptive effect as referred to in point (c) of Article 5(2), Member States shall take into account the following criteria:

(a) the number of users relying on the ***essential*** service provided by the entity***;***

(b) the dependency of other sectors ***and subsectors*** referred to in the Annex on that ***essential*** service;

(c) the impacts that incidents could have, in terms of degree and duration, on economic and societal activities, the environment ▌**,** public safety ***and security, and health of the population***;

(d) the market share of the entity in the market for such services;

(e) the geographic area that could be affected by an incident, including any cross-border impacts***, taking into account the vulnerability associated with the degree of isolation of certain types of geographic areas, such as insular regions, remote regions or mountainous areas***;

(f) the importance of the entity in maintaining a sufficient level of the ***essential*** service, taking into account the availability of alternative means for the provision of that ***essential*** service.

2. ***After the identification of the critical entities,*** Member States shall submit to the Commission ▌ the following information ***without undue delay***:

(a) the list of ***essential*** services referred to in Article 4(1);

(b) the number of critical entities identified for each sector and subsector referred to in the Annex and ***for each essential*** service ▌ referred to in ***article*** 4(1) ▌ ;

(c) any thresholds applied to specify one or more of the criteria in paragraph 1***, which can be presented as such or in aggregated form***.

They shall subsequently submit that information where necessary, and at least every four years.

3. The Commission ***shall***, after consultation of the Critical Entities Resilience Group, adopt ***non-binding*** guidelines to facilitate the application of the criteria referred to in paragraph 1, taking into account the information referred to in paragraph 2.

Article 7

Critical entities in the banking, financial market infrastructure and digital infrastructure sectors

▌

3a. Member States shall ***ensure that Article 9a and Chapters III, IV and VI do not apply*** to ***identified*** critical entities ▌ in ***the sectors referred to in points 3, 4 and 8 of the table*** in the ▌ ***Annex.*** Member States ***may adopt or maintain provisions of national law to achieve a higher level of resilience for those critical entities, provided that those national provisions are consistent with applicable Union law***.

Article 8

Competent authorities and single point of contact

1. Each Member State shall designate one or more competent authorities responsible for the correct application, and where necessary enforcement, of the rules of this Directive at national level ('competent authority'). Member States may designate an existing authority or authorities.

In respect of the critical entities in the sectors referred to in points 3 and 4 of the table in the Annex, the authorities designated as competent authorities shall, in principle, be the competent authorities referred to in Article 41 of [DORA Regulation]. In respect of the critical entities referred to in point 8 of the table in the Annex, the designated competent authorities shall, in principle, be the competent authorities designated pursuant to Article 8 of [NIS 2 Directive]. […] Member States may designate a different competent national authority for those sectors in accordance with existing national frameworks [...].

Where they designate more than one authority, they shall clearly set out the respective tasks of the authorities concerned and ensure that they cooperate effectively to fulfil their tasks under this Directive, including with regard to the designation and activities of the single point of contact referred to in paragraph 2.

2. Each Member State shall ***designate one national single point of contact, where relevant*** within ***a*** competent authority, ▌ to exercise a liaison function to ensure cross-border cooperation with ***the single points of contact*** of other Member States and ▌ the Critical Entities Resilience Group referred to in Article 16 (***"***single point of contact***"***). ***Where relevant, it could also ensure a liaison function with the Commission and cooperation with third countries.***

3. By [***five*** years and six months after entry into force of this Directive], and every ***two years*** thereafter, the single points of contact shall submit a summary report to the Commission and to the Critical Entities Resilience Group on the notifications received, including the number of notifications, the nature of notified incidents and the actions taken in accordance with Article 13(3).

3a. The Commission shall, in cooperation with the Critical Entities Resilience Group, develop a common reporting template, which the competent authorities of the Member States may use, on a voluntary basis, for the purposes of submitting summary reports as referred to in the first subparagraph.

4. Each Member State shall ensure that the competent authority ***and*** the single point of contact ***have*** the powers and the adequate financial, human and technical resources to carry out, in an effective and efficient manner, the tasks assigned to ***them***.

5. Member States shall ensure that their competent authorities, whenever appropriate, and in accordance with Union and national law, consult and cooperate with other relevant national authorities, ***including*** those in charge of civil protection, law enforcement and protection of personal data, as well as ***critical entities and*** relevant interested parties ▌.

6. Member States shall ensure that their competent authorities designated pursuant to this Article cooperate ***and exchange information*** with competent authorities designated pursuant to [the NIS 2 Directive] on cybersecurity risks ▌**,** cyber ***threats and incidents and non-cyber risks, threats and*** incidents affecting critical entities, as well as ***relevant*** measures taken by competent authorities designated under [the NIS 2 Directive] ***and this Directive***.

7. Each Member State shall notify the Commission of the designation of the competent authority and single point of contact within three months from that designation, including their ▌ tasks and responsibilities under this Directive, their contact details and any subsequent change thereto. ***Where Member States decided to appoint other authorities than those indicated under paragraph 1, second subparagrah, as the designated competent authorities in respect of the critical entities referred to in points 3, 4 and 8 of the table in the Annex, they shall also specify that to the Commission.*** Each Member State shall make public its designation of the competent authority and single point of contact.

8. The Commission shall publish a list of Member States' single points of contacts.

Article 9

Member States' support to critical entities

1. Member States shall support critical entities in enhancing their resilience. That support may include developing guidance materials and methodologies, supporting the organisation of exercises to test their resilience and providing ***advice and*** training to personnel of critical entities. ***Member States may provide financial resources to critical entities, without prejudice to applicable rules on State aid, where necessary and justified by public interest objectives.***

2. Member States shall ensure that the competent authorities cooperate and exchange information and good practices with critical entities of the sectors referred to in the Annex.

3. Member States shall ***facilitate*** voluntary information sharing between critical entities in relation to matters covered by this Directive, in accordance with Union and national law on, in particular, ***classified and sensitive information,*** competition and protection of personal data.

Article 9a

Cooperation between Member States

Member States shall engage in consultations with each other regarding critical entities whenever appropriate for the consistent application of the Directive. Such consultations shall take place in particular regarding critical entities:

(a) that use critical infrastructure which is physically connected between two or more Member States;

(b) that are part of corporate structures that are connected with, or linked to, critical entities in other Member States;

(c) that have been identified as such in one Member State and provide essential services to or in other Member States.

The consultations shall aim at enhancing the resilience of critical entities and, where possible, reducing the administrative burden for the critical entities.

Chapter III

Resilience of Critical Entities

Article 10

Risk assessment by critical entities

Member States shall ensure that critical entities assess within ***nine*** months after receiving the notification referred to in Article 5(3), and subsequently where necessary and at least every four years, on the basis of Member States' risk assessments and other relevant sources of information, all relevant risks that may disrupt their ***provision of essential services concerned***.

The risk assessment ***of the critical entities*** shall account for all relevant risks referred to in Article 4(1) which could lead to ***an incident***. It shall take into account ***dependencies*** of ***and on*** other sectors referred to in the Annex on the essential service provided by the critical entity, including in

neighbouring Member States and third countries where relevant***. Where critical entities have undertaken assessments of risk or drawn up documents pursuant to obligations in other acts of law that are relevant for the measures referred to in the first sub-paragraph, they may use those assessments*** and ***documents to meet*** the ***requirements set out in this Article. When exercising its supervisory functions, the competent authority designated pursuant to Article [8] paragraph 1 may decide to declare an existing risk assessment of a critical entity that addresses the risks and dependencies referred to in the first sub-paragraph as compliant in part or in whole with the obligations under this Article***.

Article 11

Resilience measures of critical entities

1. Member States shall ensure that critical entities take appropriate and proportionate technical***, security,*** and organisational measures to ensure their resilience***, according to the relevant information provided by Member States on the risk assessment referred to in Article 4, as well as the outcomes of the Risk Assessment referred to in Article 10***, including measures necessary to:

   (a) prevent incidents from occurring, ***duly considering*** disaster risk reduction and climate adaptation measures;

   (b) ensure adequate physical protection of ***the premises*** and ***the critical*** infrastructure ***duly considering measures such as*** fencing, barriers, perimeter monitoring tools and routines, as well as detection equipment and access controls;

   (c) ***respond to,*** resist and mitigate the consequences of incidents ***duly considering*** the implementation of risk and crisis management procedures and protocols and alert routines;

   (d) recover from incidents, ***duly considering*** business continuity measures and the identification of alternative supply chains***, to resume the provision of the essential service***;

   (e) ensure adequate employee security management, ***duly considering measures such as*** setting out categories of personnel exercising critical functions, establishing access rights to ***premises, critical*** infrastructure ▌ and ▌ sensitive information***, designating***

the categories of persons and setting up vetting procedures in accordance with Article 12, as well as laying down appropriate training requirements and qualifications. For the purposes of this point, personnel of external service providers shall be taken into account when setting out categories of personnel ***exercising critical functions***;

(f) raise awareness about the measures referred to in points (a) to (e) among relevant personnel ***duly considering training courses, information materials and exercises***.

2. Member States shall ensure that critical entities have in place and apply a resilience plan or equivalent document or documents, describing ▌ the measures pursuant to paragraph 1. Where critical entities have ***drawn up documents or*** taken measures pursuant to obligations ▌ in other acts of ▌ law that are ▌ relevant for the measures referred to in paragraph 1, they ***may use*** those measures ***and documents to meet the requirements set out in this Article. When exercising its supervisory functions, the competent authority designated pursuant to Article [8] paragraph 1 may decide to declare existing resilience-enhancing measures of a critical entity that address the technical, security and organisational measures referred to in the first paragraph in an appropriate and proportionate manner as compliant in part or in whole with the obligations under this Article.***

2a. Member States shall ensure that each critical entity designates a liaison officer or equivalent ***as point of contact with the competent authorities***.

3. Upon request of the Member State that identified the critical entity and with the agreement of the critical entity concerned, the Commission shall organise advisory missions, in accordance with the arrangements set out in Article ***15(5***), (7) and (8), to provide advice to the critical entity concerned in meeting its obligations pursuant to Chapter III. The advisory mission shall report its findings to the Commission, that Member State and the critical entity concerned.

4. The Commission ***shall, after consultation of the Critical Entities Resilience Group, adopt non-binding guidelines to further specify the technical, security and organisational measures that can be taken pursuant to paragraph 1.***

5. The Commission shall adopt implementing acts in order to set out the necessary technical and methodological specifications relating to the application of the measures referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 20(2).

Article 12

Background checks

1. Member ***states*** shall ***specify the conditions according to which*** critical entities ***are permitted, in duly reasoned cases and taking into account the risk assessment adopted pursuant to Article 4, to*** submit requests for background checks on persons who ▌***:***

(a) hold sensitive roles in or for the benefit of the critical entity, notably in relation with the resilience of the critical entity;

(b) are mandated to have direct or remote access to its premises, information or control systems including in connection with the security of the critical entity;

(c) are being considered for recruitment to positions that fall under criteria mentioned in points a) and b).

1a. These requests shall be assessed within a reasonable timeframe and processed in accordance with national legislation and procedures, as well as relevant and applicable Union law, including Regulation (EU) (EU) 2016/679 of the European Parliament and of the Council and Directive (EU) 2016/680 of the European Parliament and of the Council[35]. Such background checks shall be proportionate and strictly limited to what is necessary. They shall be carried out for the sole purpose of evaluating a potential security risk to the critical entity.

2. ***A*** background check as referred to in paragraph 1 shall***, at least***:

(a) ***corroborate*** the person's identity ▌;

(b) ***check*** criminal records ▌, on crimes relevant for ▌ a specific position ▌;

▌

[35] ***Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.***

Member States shall ***, for the purpose of obtaining*** the information on criminal records from other Member States***, use the European Criminal Records Information System (***ECRIS***)*** in accordance with the procedures set out in Council Framework Decision 2009/315/JHA, and, where relevant ***and applicable***, Regulation (EU) 2019/816 of the European Parliament and of the Council[36]. The central authorities referred to in Article 3 of that Framework Decision and in Article 3(5) of that Regulation shall provide replies to requests for such information within 10 working days from the date the request was received ***in accordance with Article 8(1) of that Framework Decision***.

▌

Article 13

Incident notification

1. Member States shall ensure that critical entities notify without undue delay the competent authority of incidents that significantly disrupt or have the potential to significantly disrupt ***the provision of essential services. Unless operationally unable to do so, an initial notification shall be submitted within 24 hours of a critical entity becoming aware of an incident, followed, where relevant, by a detailed report no later than one month thereafter. In order to determine the significance, the following parameters shall, in particular, be taken into account:***

(a) the number and share of users affected;

(b) the duration;

(c) the geographical area affected, taking into account whether the area is geographically isolated.

Where an incident has or might have a significant impact on the continuity of the provision of essential services in six Member States or more, the competent authority of the Member States affected shall notify such incidents to the Commission.

[36] OJ L 135, 22.5.2019, p. 1.

2. Notifications shall include any available information necessary to enable the competent authority to understand the nature, cause and possible consequences of the incident, including so as to determine any cross-border impact of the incident. Such notification shall not make the critical entities subject to increased liability.

▌

3. On the basis of the information provided in the notification by the critical entity, the competent authority, via ***the*** single point of contact, shall inform the single point of contact of other affected Member States if the incident has, or may have, a significant impact on critical entities and the continuity of the provision of essential services in one or more other Member States.

In so doing, the single points of contact shall, in accordance with Union law or national legislation ▌, treat the information in a way that respects its confidentiality and protects the security and commercial interest of the critical entity concerned.

4. As soon as possible upon having been notified in accordance with paragraph 1, the competent authority shall provide the critical entity ▌ with relevant ▌ follow-up ***information***, including information that could support the critical entity's effective response to the incident. ***Member States shall inform the public where they determine that it would be in the public interest to do so.***

▌

Article ***13a***

Standards

1. In order to promote the convergent implementation of this Directive, Member States shall, where useful and without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European and internationally recognised standards and technical specifications relevant to the security and resilience of critical entities.

Chapter ***IV***

Critical entities of particular European significance

Article 14

Identification of Critical entities of particular European significance

▌

2. An entity shall be considered a critical entity of particular European significance when it has been identified as a critical entity ***pursuant to article 5(1),*** it provides ***the same or similar*** essential services to or in ***six or*** more ▌ Member States and ***it*** has been notified ▌ pursuant to ***paragraph 3 of this*** Article ▌

2a. Member States shall ensure that a critical entity, following the notification referred in Article 5(3), provides information to its competent authority designated pursuant to Article 8 of this Directive, when it provides essential services to or in six or more Member States, and if so, which essential services to or in which Member States.

The Member State shall notify, without undue delay, the Commission of that information as well as the identity of the critical entity.

The Commission shall engage in consultations with the competent authorities of the Member State which identified such a critical entity and of other Member States concerned, and with the critical entity. In these consultations, each Member State shall communicate to the Commission if it deems that the services provided to it by the critical entity are essential services.

3. ***If the Commission establishes, on the basis of the consultations in paragraph 2a, that the critical entity concerned provides essential services to or in six or more Member States, it shall*** notify the entity concerned***, through its competent authority,*** that it is considered a critical entity of particular European significance, informing that entity of its obligations pursuant to this Chapter and the date from which those obligations apply to it. ***Once the competent authority is informed by the Commission of its decision to consider an entity as a critical entity of particular European importance, the competent authority shall forward the notification to the critical entity designated as of particular European significance without undue delay.***

4. The provisions of this Chapter shall apply to the critical entity of particular European significance concerned from the date of receipt of ***the*** notification ***referred to in paragraph 3***.

Article 15

Advisory Missions

1. The Member State that has identified a critical entity of particular European significance as a critical entity, may request the Commission to organise an advisory mission to assess the measures that that entity has put in place to meet its obligations pursuant to Chapter III.

1a. One or more Member States to or in which the essential service is provided, or the Commission, may also request an advisory mission referred to in paragraph 1. Upon agreement of the Member State that has identified a critical entity of particular European significance as a critical entity, the Commission shall organise such an advisory mission.

2. ***Upon reasoned*** request of one or more Member States ***to*** or ***in which the essential service is provided, or*** the Commission, the Member State ***that has identified a*** critical entity of particular European significance ***as a critical*** entity ***shall provide to*** the Commission ▌***:***

(a) the ***relevant parts*** of the risk assessment carried out pursuant to Article 10 ▌***;***

(b) ***a list of relevant*** measures taken in accordance with Article 11***;***

▌

(b) supervisory or enforcement actions, including ▌ assessments of compliance or orders issued, that its competent authority has undertaken pursuant to Articles 18 and 19 in respect of that entity.

▌

3. The advisory mission shall report its findings to the Commission, the ***Member State that has identified a*** critical entity of particular European significance ***as a critical entity, the***

Member States to or in which the essential service is provided and the entity concerned within a period of three months after the conclusion of the advisory mission.

The ***Member States to or in which the essential service is provided*** shall analyse the report and, where necessary, shall advise the Commission on whether the critical entity of particular European significance concerned complies with its obligations pursuant to Chapter III and, where appropriate, which measures could be taken to improve the resilience of that entity.

The Commission shall, based on that advice, communicate its ***opinion*** to the Member State ▌ that ***has identified a critical*** entity ***of particular European significance as a critical entity, the Member States to or in which the essential service is provided*** and that entity on whether that entity complies with its obligations pursuant to Chapter III and, where appropriate, which measures could be taken to improve the resilience of that entity.

That Member State shall ***ensure that its competent authority and the critical entity concerned*** take due account of ***that opinion*** and provide information to the Commission and the ***Member States to or in which the essential service is provided*** on ▌ measures it has taken pursuant to ***that opinion***.

4. Each advisory mission shall consist of experts from ***the Member State where the critical entity of particular European significance is located, the*** Member States ***to or in which the essential service is provided*** and of Commission representatives. ***Those*** Member States may propose candidates to be part of an advisory mission. The Commission shall***, after consultation with the Member State that has identified a critical entity of particular European significance as a critical entity,*** select and appoint the members of each advisory mission according to their professional capacity and ensuring ***where possible*** a geographically balanced representation ***from all those*** Member States***. Whenever necessary, members of the advisory mission shall have a valid and appropriate security clearance***. The Commission shall bear the costs related to the participation in the advisory mission.

The Commission shall organise the programme of an advisory mission, in consultation with the members of the specific advisory mission and in agreement with the Member State ***that has identified a*** critical entity of ***particular*** European significance ***as a critical entity***.

5. The Commission shall adopt an implementing act laying down rules on the procedural arrangements ***for the requests and their handling,*** for the conduct and reports of advisory missions ***and for the handling of the communication on the Commission's opinion and on the measures taken, duly taking into account the confidentiality and the commercial sensitivity of the information concerned***. This implementing act shall be adopted in accordance with the examination procedure referred to in Article 20(2).

6. Member States shall ensure that the critical entity of particular European significance concerned provides the advisory mission with access to ▌ information, systems and facilities relating to the provision of its essential services necessary for ***carrying out*** the ***advisory mission***.

7. The advisory mission shall be carried out in compliance with the applicable national law of the Member State where ***it takes place, respecting that Member State's responsibility for national security and protection of its security interests***.

8. When organising the advisory missions, the Commission shall take into account the reports of any inspections carried out by the Commission under Regulation (EC) 300/2008 and Regulation (EC) 725/2004 and of the reports of any monitoring carried out by the Commission under Directive 2005/65/EC in respect of the critical entity or the critical entity of particular European significance, as appropriate.

8a. The Commission shall inform the Critical Entities Resilience Group whenever an advisory mission is organised. The Member State where the advisory mission took place and the Commission shall also inform the Critical Entities Resilience Group of the main findings of the advisory mission and the lessons-learned with a view to promoting mutual learning.

Chapter V

Cooperation and Reporting

Article 16

Critical Entities Resilience Group

1. A Critical Entities Resilience Group is established with effect from [six months after the entry into force of this Directive]. It shall support the Commission and facilitate cooperation ***among Member States*** and the exchange of information on issues relating to this Directive.

2. The Critical Entities Resilience Group shall be composed of representatives of the Member States and the Commission ***holding security clearance, where appropriate***. Where relevant for the performance of its tasks, the Critical Entities Resilience Group may invite ***relevant stakeholders*** to participate in its work***. If so requested by Parliament, the Commission may also invite Parliament's experts to attend meetings of the Critical Entities Resilience Group***.

   The Commission's representative shall chair the Critical Entities Resilience Group.

3. The Critical Entities Resilience Group shall have the following tasks:

(a) supporting the Commission in assisting Member States in reinforcing their capacity to contribute to ensuring the resilience of critical entities in accordance with this Directive;

(b) ***analysing*** the strategies on the resilience of critical entities referred to in Article 3 ***in order to identify*** best practices in respect of those strategies;

(c) facilitating the exchange of best practices with regard to the identification of critical entities by the Member States in accordance with Article 5, including in relation to cross-border ***and cross sectoral*** dependencies and regarding risks and incidents;

(ca) where appropriate, contribute on issues relating to this Directive to documents concerning resilience at EU-level;

(d) contributing to the preparation of the guidelines referred to in ***Articles*** 6(3) and ***11(4) and, upon request,*** any delegated ***or*** implementing acts under this Directive ▌;

(e) ***analysing*** the summary reports referred to in Article 8(3) ***with a view to promoting the sharing of best practices on the action taken in accordance with Article 13(3)***;

(f) exchanging best practices ▌ related to the notification of incidents referred to in Article 13;

(g) ***discuss*** the ***summary*** reports of advisory missions ***and lessons-learned*** in accordance with Article 15***(9***);

(h) exchanging information and best practices on ***innovation,*** research and development relating to the resilience of critical entities in accordance with this Directive;

(i) where relevant, exchanging information on matters concerning the resilience of critical entities with relevant Union institutions, bodies, offices and agencies.

4. By [24 months after entry into force of this Directive] and every two years thereafter, the Critical Entities Resilience Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks, which shall be consistent with the requirements and objectives of this Directive.

5. The Critical Entities Resilience Group shall meet regularly and at least once a year with the Cooperation Group established under [the NIS 2 Directive] to ***facilitate both*** cooperation and exchange of information.

6. The Commission may adopt implementing acts laying down procedural arrangements necessary for the functioning of the Critical Entities Resilience Group***, pursuant to the provisions of Article 1.4***. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 20(2).

7. The Commission shall provide to the Critical Entities Resilience Group a summary report of the information provided by the Member States pursuant to Articles 3(3) and 4(4) by ***four*** years ▌ after entry into force of this Directive ▌ and subsequently where necessary and at least every four years.

Article 17 ▌

Commission support to competent authorities and critical entities

1. The Commission shall, where appropriate, support Member States and critical entities in complying with their obligations under this Directive ▌***. The Commission shall prepare*** a Union-level overview of cross-border and cross-sectoral risks to the provision of essential services, ***organise*** the advisory missions referred to in Articles 11(3) and ▌ ***15*** and ***facilitate*** information exchange among ***Member States and*** experts across the Union.

2. The Commission shall complement Member States' activities referred to in Article 9 by developing best practices***, guidance materials*** and methodologies, and by developing cross-border training activities and exercises to test the resilience of critical entities.

2a. The Commission shall inform Member States about financial resources at EU level available to Member States for enhancing the resilience of critical entities.

Chapter VI

Supervision and enforcement

Article 18

Implementation and enforcement

1. In order to assess the compliance of the entities that the Member States identified as critical entities pursuant to Article 5 with the obligations pursuant to this Directive, they shall ensure that the competent authorities shall have the powers and means to:

   (a) conduct on-site inspections of ***the critical infrastructure and*** the premises that the critical entity uses to provide its essential services, and off-site supervision of critical entities' measures pursuant to Article 11;

   (b) conduct or order audits in respect of those entities.

2. Member States shall ensure that the competent authorities have the powers and means to require, where necessary for the performance of their tasks under this Directive, that the entities that they identified as critical entities pursuant to paragraph 5 provide, within a reasonable time period set by those authorities:

   (a) the information necessary to assess whether the measures taken by those ***entities*** to ensure ***their*** resilience meet the requirements of Article 11;

   (b) evidence of the effective implementation of those measures, including the results of an audit conducted by an independent and qualified independent auditor selected by that entity and conducted at its expense.

   When requiring that information, the competent authorities shall state the purpose of the requirement and specify the information required.

3. Without prejudice to the possibility to impose penalties in accordance with Article 19, the competent authorities may, following the supervisory actions referred to in paragraph 1, or the assessment of the information referred to in paragraph 2, order the critical entities concerned to take the necessary and proportionate measures to remedy any identified infringement of this Directive, within a reasonable time period set by those authorities, and to provide to those authorities information on the measures taken. Those orders shall take into account, in particular, the seriousness of the infringement.

4. Member State shall ensure that the powers provided for in paragraphs 1, 2 and 3 can only be exercised subject to appropriate safeguards. Those safeguards shall guarantee, in

particular, that such exercise takes place in an objective, transparent and proportionate manner and that the rights and legitimate interests***, such as the protection of trade- and business secrets,*** of the critical entities affected are duly safeguarded, including their rights to be heard, of defence and to an effective remedy before an independent court.

5. Member States shall ensure that, when a competent authority assesses the compliance of a critical entity pursuant to this Article, it shall inform the competent authorities of the Member State concerned designated under the [the NIS 2 Directive] and may request those authorities to ***exercise their supervisory and enforcement powers in relation to an essential entity under*** the ***scope*** of ***[NIS 2 Directive] that is also identified as critical under this Directive***, and cooperate and exchange information for this purpose.

Article 19

Penalties

Member States shall lay down the rules on penalties applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall notify those provisions to the Commission by [***21 months*** after entry into force of this Directive] at the latest and shall notify it without delay of any subsequent amendment affecting them.

Chapter VII

Final provisions

Article 20

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Article 21

Exercise of the delegation

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

2. The power to adopt delegated acts referred to in Article ***4(1***) shall be conferred on the Commission for a period of five years from date of entry into force of this Directive or any other date set by the co-legislators.

3. The delegation of power referred to in Article ***4(1***) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

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

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

6. A delegated act adopted pursuant to Article ***4(1***) 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 22

Reporting and review

By [54 months after the entry into force of this Directive], the Commission shall submit a report to the European Parliament and to the Council, assessing the extent to which ***each*** Member ***State has*** taken the necessary measures to comply with this Directive.

The Commission shall periodically review the functioning of this Directive, and report to the European Parliament and to the Council. The report shall in particular assess the impact and added value of this Directive on ensuring the resilience of critical entities and whether the ***Annex*** of the Directive should be ***modified***. The first report shall be submitted by [***6*** years ***and 5 months*** after the entry into force of this Directive] ▌***. For that purpose, the Commission shall take into account relevant documents of the Critical Entities Resilience Group***.

Article 23

Repeal of Directive 2008/114/EC

Directive 2008/114/EC is repealed with effect from [date of ***transposition*** of this Directive].

References to the repealed Directive shall be construed as references to this Directive.

Article 24

Transposition

1. Member States shall adopt and publish, by [***21*** months after entry into force of this Directive] at the latest, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith communicate to the Commission the text of those provisions.

   They shall apply those provisions from [***21 months*** after entry into force of this Directive + one day].

   When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 25

Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

Article 26

Addressees

This Directive is addressed to the Member States.

Done at Brussels,

For the European Parliament *For the Council*

The President *The President*

ANNEX

Sectors, subsectors and ***categories of entities***

Sectors	Subsectors	***Categories of entities***
1. Energy	(a) Electricity	— Electricity undertakings referred to in point (57) of Article 2 of Directive (EU) 2019/944[1], which carry out the function of 'supply' referred to in point (12) of Article 2 of that Directive
		— Distribution system operators referred to in point (29) of Article 2 of Directive (EU) 2019/944
		— Transmission system operators referred to in point (35) of Article 2 of Directive (EU) 2019/944
		— Producers referred to in point (38) of Article 2 of Directive (EU) 2019/944
		— Nominated electricity market operators referred to in point 8 of Article 2 of Regulation (EU) 2019/943[2]

[1] Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019, p.125.

[2] Regulation (EU) 2019/943 of the European Parliament and of the Council on the internal market for electricity (OJ L 158, 14.6.2019, p. 54).

Sectors	Subsectors	***Categories of entities***
		— Electricity market participants referred to in point (25) of Article 2 of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services referred to in points (18), (20) and (59) of Article 2 of Directive (EU) 2019/944
	(b) District heating and cooling	— District heating and cooling referred to in point (19) of Article 2 of the Directive (EU) 2018/2001[3] on the promotion of the use of energy from renewable sources
	(c) Oil	— Operators of oil transmission pipelines
		— Operators of oil production, refining and treatment facilities, storage and transmission
		— Central oil stockholding entities referred to in point (f) of Article 2 of Council Directive 2009/119/EC[4]

[3] Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (OJ L 328, 21.12.2018, p. 82).

[4] Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products (OJ L 265, 9.10.2009, p.9).

Sectors	Subsectors	***Categories of entities***
	(d) Gas	— Supply undertakings referred to in point (8) of Article 2 of Directive (EU) 2009/73/EC[5]
		— Distribution system operators referred to in point (6) of Article 2 of Directive (EU) 2009/73/EC
		— Transmission system operators referred to in point (4) of Article 2 of Directive (EU) 2009/73/EC
		— Storage system operators referred to in point (10) of Article 2 of Directive (EU) 2009/73/EC
		— LNG system operators referred to in point (12) of Article 2 of Directive (EU) 2009/73/EC
		— Natural gas undertakings referred to in point (1) of Article 2 of Directive (EU) 2009/73/EC
		— Operators of natural gas refining and treatment facilities
	(e) Hydrogen	— Operators of hydrogen production, storage and transmission

[5] Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (OJ L 211, 14.8.2009, p. 94).

Sectors	Subsectors	***Categories of entities***
2. Transport	(a) Air	— Air carriers referred to in point (4) of Article 3 of Regulation (EC) No 300/2008[6] ***used for commercial purposes***
		— Airport managing bodies referred to in point (2) of Article 2 of Directive 2009/12/EC[7] , airports referred to in point (1) of Article 2 of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013[8], and entities operating ancillary installations contained within airports
		— Traffic management control operators providing air traffic control (ATC) services referred to in point (1) of Article 2 of Regulation (EC) No 549/2004[9]

6 Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p.72).

7 Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges (OJ L 70, 14.3.2009, p.11).

8 Regulation (EC) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU (OJ L 348, 20.12.2013, p.1).

9 Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation) (OJ L 96, 31.3.2004, p.1).

Sectors	Subsectors	***Categories of entities***
	(b) Rail	— Infrastructure managers referred to in point (2) of Article 3 of Directive 2012/34/EU[10]
		— Railway undertakings referred to in point (1) of Article 3 of Directive 2012/34/EU ***and*** operators of service facilities referred to in point (12) of Article 3 of Directive 2012/34/EU
	(c) Water	— Inland, sea and coastal passenger and freight water transport companies, referred to for maritime transport in Annex I to Regulation (EC) No 725/2004[11], not including the individual vessels operated by those companies

[10] Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (OJ L 343, 14.12.2012, p.32).

[11] Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p.6).

Sectors	Subsectors	***Categories of entities***
		— Managing bodies of ports referred to in point (1) of Article 3 of Directive 2005/65/EC[12], including their port facilities referred to in point (11) of Article 2 of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports
		— Operators of vessel traffic services referred to in point (o) of Article 3 of Directive 2002/59/EC[13] of the European Parliament and of the Council
	(d) Road	— Road authorities referred to in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962[14] responsible for traffic management control, ***excluding public entities for whom traffic-management or operators of intelligent transport systems is only a non-essential part of their general activity***
		— Operators of Intelligent Transport Systems referred to in point (1) of Article 4 of Directive 2010/40/EU[15]

12 Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28).

13 Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p.10).

14 Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU–wide real–time traffic information services (OJ L 157, 23.6.2015, p. 21).

15 Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1).

Sectors	Subsectors	*Categories of entities*
	(e) public transport	— ***Public transport service operators as referred to in Article 2, point (d), of Regulation (EC) No 1370/2007 of the European Parliament and of the Council[16].***
3. Banking		— Credit institutions referred to in point (1) of Article 4 of Regulation (EU) No 575/2013[17]
4. Financial market infrastructures		— Operators of trading venues referred to in point (24) of Article 4 of Directive 2014/65/EU[18]
		— Central counterparties (CCPs) referred to in point (1) of Article 2 of Regulation (EU) No 648/2012[19]

16 ***Regulation (EC) No 1370/2007 of the European Parliament and of the Council of 23 October 2007 on public passenger transport services by rail and by road and repealing Council Regulations (EEC) Nos 1191/69 and 1107/70 (OJ L 315, 3.12.2007, p. 1).***

17 Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

18 Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

19 Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).

Sectors	Subsectors	***Categories of entities***
5. Health		— Healthcare providers referred to in point (g) of Article 3 of Directive 2011/24/EU[20]
		— EU reference laboratories referred to in Article 15 of Regulation [XX] on serious cross borders threats to health[21]
		— Entities carrying out research and development activities of medicinal products referred to in Article 1 point 2 of Directive 2001/83/EC[22]
		— Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2
		— Entities manufacturing medical devices considered as critical during a public health emergency ('the public health emergency critical devices list') referred to in Article 22 ***of Regulation (EU) 2022/123[23]***
		— ***Entities holding a distribution authorisation as referred to in Article 79 of Directive 2001/83/EC***

20 Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross–border healthcare (OJ L 88, 4.4.2011, p. 45).

21 [Regulation of the European Parliament and of the Council on serious cross-border threats to health and repealing Decision No 1082/2013/EU, reference to be updated once the proposal COM(2020) 727 final is adopted].

22 Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the community code relating to medicinal products for human use (OJ L 311, 28.11.2001, p.67).

23 ***Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022 on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices (OJ L 20, 31.1.2022, p. 1–37)].***

Sectors	Subsectors	***Categories of entities***
6. Drinking water		— Suppliers and distributors of water intended for human consumption referred to in point (1)(a) of Article 2 of Directive (EU) 2020/2184[24] but excluding distributors for whom distribution of water for human consumption is only ***non-essential*** part of their general activity of distributing other commodities and goods
7. Waste water		— Undertakings collecting, disposing or treating urban, domestic and industrial waste water referred to in points (1) to (3) of Article 2 of Council Directive 91/271/EEC[25], ***but excluding undertakings for whom collecting, disposing or treating of urban, domestic and industrial waste water is only a non-essential part of their general activity***

[24] ***Directive (EU) 2020/2184 of the European Parliament and of the Council of 16 December 2020 on the quality of water intended for human consumption (recast) (OJ L 435, 23.12.2020, p. 1–62)].***

[25] Council Directive 91/271/EEC of 21 May 1991 concerning urban waste water treatment (OJ L 135, 30.5.1991, p.40).

Sectors	Subsectors	***Categories of entities***
8. Digital infrastructure		— Providers of Internet Exchange Point [referred to in point (X) of Article 4 of NIS 2 Directive]
		— DNS service providers [referred to in point (X) of Article 4 of NIS 2 Directive], ***excluding operators of root name servers***
		— TLD name registries [referred to in point (X) of Article 4 of NIS 2 Directive]
		— Providers of Cloud computing service [referred to in point (X) of Article 4 of NIS 2 Directive]
		— Providers of Data centre service [referred to in point (X) of Article 4 of NIS 2 Directive]
		— Providers of Content delivery network [referred to in point (X) of Article 4 of NIS 2 Directive]
		— Trust service providers referred to in point (19) of Article 3 of Regulation (EU) No 910/2014[26]
		— Providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972[27] or providers of electronic communications services within the meaning of point (4) of Article 2 of Directive (EU) 2018/1972 insofar as their services are publicly available

[26] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p.73).

[27] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communication Code (OJ L 321, 17.12.2018, p. 36).

Sectors	Subsectors	***Categories of entities***
9. Public administration ***entities excluding the judiciary, parliaments and central banks***		— Public administration entities ▌ of central governments ***as defined by a Member State in accordance with national law*** ▌
10. Space		— Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks within the meaning of point (8) of Article 2 of Directive (EU) 2018/1972
10a. Food production, processing and distribution		***– Food businesses referred to in point (2) of Article 3 of Regulation (EC) No 178/2002[28] engaged exclusively in logistics and wholesale distribution and large scale industrial production and processing***

[28] Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (OJ L 31, 1.2.2002, p. 1).