Council of the European Union

Brussels, 7 December 2021
(OR. en)

14594/21

Interinstitutional File:
2020/0365 (COD)

PROCIV 160	RELEX 1041
ENV 956	ENER 539
JAI 1329	HYBRID 76
SAN 717	TRANS 720
COSI 243	CYBER 319
CHIMIE 124	TELECOM 450
ENFOPOL 481	ESPACE 121
RECH 549	ATO 88
CT 166	CSC 427
DENLEG 97	ECOFIN 1194
COTER 164	

'I/A' ITEM NOTE

From:	Presidency
To:	Permanent Representatives Committee/Council
No. Cion doc.:	14262/20 + ADD1
Subject:	Proposal for a Directive of the European Parliament and the of the Council on the resilience of critical entities – General Approach

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 CER Directive proposal was discussed in the Informal VTC of the Ministers of Home Affairs, which took place on 12 March 2021, and in the Justice and Home Affairs Council on 7-8 June 2021. In both instances, ministers had an exchange of views in public session based on Presidency framing documents[8]. Ministers welcomed the proposal's key objectives, including the overall objective of enhancing the Union's resilience, as well as the ambition to enlarge the scope of the preceding ECI Directive.

---

3 14972/19
4 A9-0289/2021
5 8416/21
6 10580/21
7 11280/21
8 6630/21, 8969/21

9. In its conclusions of 21-22 October 2021, the European Council called for advancing work on the proposal for on the Directive on the resilience of critical entities.[9]

10. The changes in the annexed text are indicated by **bold underlining** and ~~strike-through~~ as compared to the relevant parts of the Commission proposal.

II. WORK WITHIN THE COUNCIL PREPARATORY BODIES

11. In the Council, the examination of the proposal has been carried out in the specific formation of the Working Party on Civil Protection, dedicated to the Critical Entities Resilience Directive (hereinafter: PROCIV CER). The examination of the proposal started during the Portuguese Presidency on 18 February, where the Commission presented the proposal and its impact assessment and gave a comprehensive explanation to general questions asked by the Member States.

12. During the Portuguese Presidency, 7 informal meetings of the members of PROCIV CER were held, dedicated to the presentation and read-through of the proposal. A Presidency progress report, setting out the work done in the Council's preparatory bodies and providing an account on the state of play in the examination of the proposal was submitted to the JHA Council of 7-8 June 2021.[10]

13. The work has since continued during the Slovenian Presidency with the objective of adopting a General Approach before the end of 2021. The Slovenian Presidency dedicated five informal meetings of the members of PROCIV CER to the discussion of six Presidency compromises on CER. In addition, the Presidency organised numerous informal bilateral discussions with Member States. A Presidency progress report, setting out the work done in the Council's preparatory bodies and providing an account on the state of play in the examination of the proposal was submitted to the JHA Council of 9-10 December 2021.[11]

---

9 EUCO 17/21
10 8969/21
11 14352/21

14. Under the Slovenian Presidency, discussions at the informal meetings of the members of PROCIV CER focused, *inter alia*, on the suitability of the legal basis, the exclusion clause concerning national security and defence, an equivalence regime, the content of strategies and risk assessments to be developed by Member States and critical entities, the process for identification of critical entities, the resilience measures to be adopted by critical entities, cooperation between Member States, background checks and the identification process and advisory missions regarding the critical entities of particular European significance. A further key issue of debate was the interaction of the CER Directive with other Union legislation, notably with the proposal on a Directive on measures for a high common level of cybersecurity across the Union ("the NIS2 Directive") and the proposal on the Regulation on digital operational resilience for the financial sector (the "DORA Regulation").

15. In total, six partial or full compromise proposals were prepared by the Slovenian Presidency, based on the written comments and non-papers received from Member States.

16. The latest revision of the Presidency compromise proposal was discussed in an informal meeting of the members of PROCIV CER on 1 December 2021, followed up by an informal written consultation. Delegations welcomed the compromise text in view of submitting a consolidated text for COREPER approval and subsequent adoption by the Council.

III. SUBSTANCE

17. Based on the discussions at Working Party level, the following items have been identified as the main political issues:

a) Relationship with NIS2 Directive (including Article 7)

Member States stressed the need for alignment between the CER and other pieces of Union legislation currently being negotiated, notably NIS2 and DORA. Noteworthy, in a clear separation of scope, NIS2 addresses the resilience in the face of cyber threats, while CER addresses the resilience in the face of non-cyber threats. In addition, DORA addresses the digital operational resilience for the financial sector.

Member States also highlighted the need to avoid over-burdening the critical entities. In that respect, the compromise proposal retains the design of the Commission proposal in which large parts of the Directive do not apply to critical entities in the sectors of banking, financial market infrastructure and digital infrastructure. The rationale behind this decision is that Union legislative proposals of NIS2 and DORA, currently under negotiation, will demand an equivalent level of resilience from obliged entities. The Presidency kept a careful eye on the development of the compromise proposals of the other two legislations to promote alignment. Other important additions in the compromise proposal are related to cooperation arrangements between the competent authorities under the respective legal acts.

Furthermore, the compromise proposal aligned the scope of CER (Annex) and that of the General Approach of NIS2 (their Annex I). Due to the specificities of both Directives, the precise shape chosen for the alignment was the following: all the sectors included in CER Annex were as a minimum also to be present in the Annex I of NIS2, which included further sectors not covered in CER. This alignment reflected that NIS2 is at a different stage than CER as it already builds on the implementation of the current Directive on security of network and information systems ("the NIS Directive")[12].

The concept of "entities equivalent to critical entities" (used in the Commission proposal to describe critical entities in the sectors of banking, financial market infrastructure and digital infrastructure) is eliminated as it was thought unnecessary. In the compromise proposal, the critical entities in the three sectors of relevance are labelled as "critical entities" and assimilated to those in other sectors in scope. However, without creating a special category of entities, the compromise acknowledges that clearly specified provisions of CER do not apply to the critical entities in those three sector (Article 7).

b) Scope (regarding the economic sectors in the Annex to the Directive)

The Member States generally welcomed the enlargement of the scope from the preceding ECI Directive, which only covered energy and transport, to a wide range of sectors. However, a significant number of Member States found the inclusion of the public administration sector in the scope of the Directive as problematic because it is very distinct from the other economic sectors in scope. Therefore, the compromise proposal does not include it. The compromise proposal retains however a review mechanism (Article 22) which would allow to assess the impact and added value of the Directive and whether the scope should be modified at a later stage.

[12] Directive 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

c) Exclusion clause (Article 1.5)

Member States wished to clarify in an exclusion clause that the Directive does not apply to entities that mainly carry out activities in the areas of defence, national security, public security or law enforcement or to activities concerning national security or defence. The judiciary, parliaments and central banks are also excluded. The exclusion clause is in line with the similar one agreed in the General Approach of the NIS2 Directive.

d) The interaction with sectoral legislation

Beyond the relationship with NIS2 and DORA, Member States also stressed the need to clarify and refine the equivalence regime of CER regarding existing national and Union law. The compromise proposal provided further clarification, notably with the modifications to recital 7, Articles 1.3, 10 and 11.2. Regarding risk assessments and resilience measures, Member States may, under a set of conditions, recognise equivalence, in whole or in part, between existing measures and CER obligations.

e) Cooperation among two or more Member States (Article 9a)

The compromise proposal adds a new framework for cooperation among Member States, not initially foreseen in the Commission's proposal. In the compromise proposal, Member States have to engage in consultations with each other when two or more Member States 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. Before the addition of this new type of cooperation, the Directive provided great deal of detail about the cooperation regarding critical entities of European significance but it did not foresee a framework for cases in which the relevant Member States were less than nine.

f) Resilience Measures (Article 11)

Following requests by Member States, the compromise proposal modified the Commission's proposal to provide more flexibility for the Member States when establishing the resilience measures that the critical entities would need to undertake. Among other reasons, this was done in order to be able to adapt the resilience measures to the specific national circumstances.

g) Background checks (Article 12)

Member States raised concerns, including legal ones, regarding the reference to background checks in the Commission's proposal. The compromise proposal modified that reference so that Member States may receive and assess requests for background checks from the critical entities if they so decide. The importance of background checks in personnel security was generally highlighted by Member States. Member States considered that background checks should be processed in accordance with national law and procedures.

h) Critical entities of particular European significance (Articles 14 and 15)

Member States welcomed the category of critical entities of particular European significance but the discussions confirmed that further clarity was needed on the process of identifying those entities as well as regarding their related advisory missions. The compromise proposal provides those added specifications, strengthening the role of the European Commission in the identification process. Regarding advisory missions, the compromise proposal added also further clarity and, among other things, enhanced the role of the Member State where the critical entity of particular European significance is located as well as that of the Member States to or in which the essential service is provided.

IV. CONCLUSION

18. The COREPER therefore is invited to reach agreement on the compromise text presented by the Presidency as set out in the Annex. COREPER is also invited to submit it to the Council (Environment) for adopting a General Approach at its meeting of 20 December 2021 as well as to invite the Presidency to conduct negotiations with the European Parliament on the basis of this mandate.

ANNEX

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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[13],

Having regard to the opinion of the Committee of the Regions[14],

Acting in accordance with the ordinary legislative procedure[15],

[13] OJ C , , p. .
[14] OJ C […], […], p. […].
[15] Position of the European Parliament […] and of the Council […].

Whereas:

(0) **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 inderdependent Union economy. The smooth operation of each critical entity heavily depends on its level of preparedness and resilience, enabling it to continue or to rapidly resume performing its activity whenever disruptions occur. It is therefore essential to set out a Union-wide framework aiming both at enhancing the resilience of critical entities in the internal market by laying down a minimal harmonised set of obligations and at assisting them through coherent, dedicated support and supervision measures.**

(1) Council Directive 2008/114/EC[16] 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 focused exclusively on the protection of such infrastructures. However, the evaluation of Directive 2008/114/EC conducted in 2019[17] 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, the role and duties of individual entities as providers of services essential to the functioning of the internal market are better defined and coherent, Union-wide rules are adopted to enhance** the resilience of critical entities~~, that is,~~**. As such, critical entities should be in a position to reinforce** their ability to **prevent, protect against, respond to, resist,** mitigate, absorb, accommodate ~~to~~ and recover from incidents that have the potential to disrupt the ~~operations of the critical entity~~ **provision of essential services**.

---

16 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).

17 SWD(2019) 308.

(2) **Currently,** ~~Despite existing~~ **while a number of** measures at Union[18] and national level aim~~ed~~ at supporting the protection of critical infrastructures in the Union, the entities operating those infrastructures ~~are not~~ **could be legally better mandated and better** ~~adequately~~ equipped to address ~~current and anticipated future~~ risks to their operations that may result in disruptions of the provision of **essential** services ~~that are essential for the performance of vital societal functions or economic activities~~. This is due to a dynamic threat landscape**,** ~~with~~ **including** an evolving terrorist threat**,** and growing interdependencies between infrastructures and sectors, as well as an increased physical risk due to natural disasters and climate change, which ~~increases~~ **intensifies** the frequency and scale of extreme weather events and brings long-term changes in average climate ~~that can reduce the capacity and efficiency of certain infrastructure types if resilience or climate adaptation measures are not in place~~. Moreover**, the internal market is characterised by fragmentation in respect of the identification of critical entities, as** relevant sectors and types of entities are not recognised consistently as critical in all Member States.

18 European Programme for Critical Infrastructure Protection (EPCIP).

(3) Those growing interdependencies 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, health, ~~certain aspects of public administration,~~ as well as space**. 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 Community law. The space sector is concerned,** in as far as the provision of certain services depending on ground-based infrastructures that are owned, managed and operated either by Member States or by private parties ~~is concerned~~, therefore not covering infrastructures owned, managed or operated by or on behalf of the Union as part of its space programmes. These interdependencies mean that any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the internal market. The COVID-19 pandemic has shown the vulnerability of our increasingly interdependent societies in the face of 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~~ **resilience-enhancing** requirements on these entities not only 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. 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. **It also results in an uneven playing field and disincentives to operate across borders.**

(5) It is therefore necessary to lay down harmonised minimum rules to ensure the provision of essential services in the internal market and enhance the resilience of critical entities.

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

(7) ~~Certain sectors of the economy such as energy and transport are already regulated or may be regulated in the future by sector-specific acts of Union law that contain rules related 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, those sector-specific measures should be complemented by the ones provided for in this Directive, which creates an overarching framework that addresses critical entities' resilience in respect of all hazards, that is, natural and man-made, accidental and intentional~~.

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 the provisions as set out in this Directive. On that basis, national competent authorities should be able to decide to exclude those critical entities from their supervisory objectives and plans under this Directive, in line with the risk based approach and with a view to alleviate the burden on those critical entities. Member States should be empowered to decide the regime applicable to risk assessment and resilience measures if they are at least equivalent to those of this Directive. Member States should nevertheless include all the sectors listed in the Annex in their strategy for reinforcing the resilience of critical entities, the risk assessment and the support measures pursuant to Chapter II and be able to identify critical entities in those sectors where the applicable conditions have been met.

(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[19] [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 those requirements are 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. Member States should nevertheless include all the sectors listed in the Annex in their strategy for reinforcing the resilience of critical entities, the risk assessment and the support measures pursuant to Chapter II and be able to identify critical entities in those sectors where the applicable conditions have been met, taking into account the particular regime for entities in the banking, financial market infrastructure and digital infrastructure sector.~~

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

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 shall be done carefully and with particular attention to the transmission channels and storage capacities that will be used by the relevant stakeholders.

(9a) This Directive should not be deemed to affect the competences of Member States and of their authorities in terms of administrative autonomy, organisation and functioning of the judiciary, parliaments or central banks, or affect their responsibility to safeguard national interest, particularly concerning public security, defence and national security. Moreover, this Directive should not apply to any entity, either public or private, that mainly carries out activities in the areas of defence, national security, public security or law enforcement. It should also not apply to the activities of entities conducted in these areas. Member States should perform an individual assessment of entities that meet the criteria for being identified as a critical entity but also mainly carry out activities in the areas of national security, defence, public security or law enforcement. Upon that assessment of these specific activities, entities would be granted the benefit of the regime established by this Directive or fall outside of its scope. No Member State is to be obliged to supply information the disclosure of which would be contrary to the essential interests of its public security. National or Union rules for protecting classified information, non-disclosure agreements, and informal non-disclosure agreements are of relevance.

(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. **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 this, Member States should ensure that their ~~cybersecurity~~ strategies provide for a policy framework for enhanced coordination between the competent authority under this Directive and 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 cyber threats~~ and the exercise of supervisory tasks.

(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 ~~all~~ relevant natural and man-made risks that may affect the provision of essential services, including accidents, natural disasters, public health emergencies such as pandemics, **hybrid threats** ~~and~~ **or other** antagonistic threats, including terrorist offences. 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 ~~the~~ **their** resilience requirements ~~of this Directive~~.

(12) In order to ensure that all relevant entities are subject to those requirements 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 **exercise their decision making powers, adequately reflecting the role and importance of these entities as providers of services on their territory** ~~reflect national specificities~~. Therefore, criteria to identify critical entities should be laid down. In the interest of effectiveness~~, efficiency, consistency~~ and legal certainty, appropriate rules should also be set **out** on notification and cooperation relating to, as well as the legal consequences of, such identification. In order to enable the Commission to assess the correct application of this Directive, Member States should submit to the Commission, in a manner that is as ~~detailed and~~ specific as possible, relevant information and, in any event, the list of essential services, the number of critical entities identified for each sector and subsector referred to in the Annex ~~and the essential service or services that each entity provides~~ and, **if used,** ~~any~~ thresholds ~~applied~~, **which can 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 **by the Member States** to determine the significance of a disruptive effect produced by such incidents **taking into account the criteria of Article 6(1)**. Those criteria should build on the criteria provided in Directive (EU) 2016/1148 of the European Parliament and of the Council[20] in order to capitalise on the efforts carried out by Member States to identify those operators and the experience gained in this regard.

[20] 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).

(**13a) Pursuant to sectoral Union law provisions, entities in the banking, financial market infrastructure and digital infrastructure sectors which may qualify as critical entities under this Directive are required to assess relevant risks, take measures to ensure their resilience and notify incidents. Given that those requirements are at least equivalent to the corresponding obligations laid down in this Directive, the provisions of Article 9a and Chapters III to V should not apply to those entities, so as to avoid duplication and unnecessary burdens on the entities. By consequence, the specific provisions on supervision and enforcement set out in Chapter VI should not be applicable either to those entities. However, in order to reinforce the resilience of the internal market as a whole and maintain the coherence and comprehensive character of the Member States' competent authorities efforts and oversight, 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 also be applicable in those specific sectors. Moreover, Member States should still identify which entities in those sectors qualify as critical entities, taking into account the particular regime for entities in the banking, financial market infrastructure and digital infrastructure sectors.**

(13b) Moreover, with the same aim of avoiding duplication and unnecessary burdens on critical entities, this Directive should establish a generally applicable equivalence regime. Thus, in a set of clearly identified areas, measures that are equivalent to the measures pursuant to this directive and already taken by critical entities belonging to any sector in order to comply with their obligations under sector-specific acts of Union law can be recognised as equivalent by Member States. Accordingly, Member States should be able to exempt critical entities, in respect of recognised equivalent measures, from taking the specific measures required under this Directive.

(14) **Directive XXXX/XXXX [NIS2 Directive] requires entities to take appropriate technical and organizational measures to manage the risks posed to the security of network and information systems which those providers use in the provision of their services as well as to notify significant incidents and cyber threats. Since threats to the security of network and information systems can have different origins, therefore [NIS2 Directive] applies an "all-hazard" approach that includes the protection of network and information systems and their physical environment. The** entities pertaining to the digital infrastructure sector are in essence based on network and information systems and **therefore the obligations imposed on those entities by [the NIS2 Directive] address in a comprehensive manner the physical security of such systems as part of their cybersecurity risk management and reporting obligations.** ~~fall within the scope of the NIS 2 Directive, which addresses the physical security of such systems as part of their cybersecurity risk management and reporting obligations. Since those matters are covered by the NIS 2 Directive, the obligations of this Directive do not apply to such entities.~~ However, considering the importance of the services provided by entities in the digital infrastructure sector ~~for the provision of other essential services~~ **to critical entities belonging to all other relevant economic sectors**, Member States should identify, based on the criteria and using the procedure provided for in this Directive *mutatis mutandis*, entities pertaining to the digital infrastructure sector **as critical entities.** ~~that should be treated as equivalent to critical entities for the purposes of Chapter II only, including the provision on Member States' support in enhancing the resilience of these entities. Consequently, such entities should not be subject to the obligations laid down in Chapters III to VI. Since the obligations for critical entities laid down in Chapter II to provide certain information to the competent authorities relate to the application of Chapters III and IV, those entities should not be subject to those obligations either.~~

(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[21], Directive 2014/65/EU of the European Parliament and of the Council[22] and Regulation (EU) No 600/2014 of the European Parliament and of the Council [23] as well as Regulation (EU) No 575/2013 of the European Parliament and of the Council[24] and Directive 2013/36/EU of the European Parliament and of the Council[25]. The ~~Commission has recently proposed to complement this~~ **legal** framework **will be 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")[26]], which lays down requirements for financial firms to manage ICT risks, including the protection of physical ICT infrastructures.

---

21 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).

22 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).

23 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).

24 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).

25 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).

26 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.

Since the resilience of entities listed in points 3 and 4 of the Annex is comprehensively covered by the EU financial services acquis, those entities should also**, similar to entities in the digital infrastructure sector,** be ~~treated as equivalent to~~ **identified as** critical entities **exclusively** for the purposes of ~~Chapter II~~ **Articles 1-9** of this Directive ~~only~~. To ensure a consistent application of the operational risk and digital resilience rules in the financial sector, Member States' support to enhancing the overall resilience of financial entities equivalent to critical entities ~~should~~ **could** be ensured by the authorities designated pursuant to Article 41 of [DORA Regulation] **or those designated persuant to this Directive**, and subject to the procedures set out in ~~that~~ **the applicable** legislation in a **coherent** ~~fully harmonised~~ manner.

(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, ~~within one of the authorities it designated as competent authority under this Directive, a~~ **one national** single point of contact responsible for coordinating issues related to the resilience of critical entities and cross-border cooperation at Union level in this regard.

(18) ~~Given that under the NIS 2 Directive entities identified as critical entities, as well as identified entities in the digital infrastructure sector that are to be treated as equivalent under the present Directive are subject to the cybersecurity requirements of the NIS 2 Directive, t~~ **T**he competent authorities designated under ~~the two Directives~~ **this Directive and those designated under [NIS 2 Directive]** should cooperate **and exchange information nationally**, ~~particularly~~ in relation to cybersecurity **risks, cyber threats and incidents** and **non-cyber** risks**, threats** and incidents affecting ~~those entities~~ **critical entities as well as on relevant measures taken by competent authorities designated under [the NIS 2 Directive] and this Directive.**

(19) Member States should support critical entities in strengthening their resilience, in compliance with their obligations under this Directive, without prejudice to the entities' own legal responsibility to ensure such compliance. 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. Moreover, given the interdependencies between entities and sectors, Member States should ~~establish information sharing tools to support~~ **facilitate** voluntary information sharing 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 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 the 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.

(20) ~~In order to be able to ensure their resilience, c~~ **C**ritical entities should have a comprehensive understanding of ~~all~~ relevant risks to which they are exposed and **a duty to** analyse those risks. To that aim, they should carry out risks assessments, whenever necessary in view of their particular circumstances and the evolution of those risks, yet in any event every four years. The risk assessments by critical entities should be based on the risk assessment carried out by Member States. **If critical entities have already conducted an assessment of these risks and dependencies as set out in Article 10 under other acts of Union or national law, Member States may recognise equivalence, in whole or in part, of these exisiting risk assessments.**

(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 ~~to~~ and recover from an incident. ~~Although~~ **While** critical entities should take measures ~~on all points specified in this Directive,~~ **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 ~~those~~ **the** measures **they take**, with a level of detail to sufficiently achieve 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. Such equivalent document or documents may be drawn up in accordance with **national law or with** requirements and standards developed in the context of international agreements on physical protection to which Member States are parties, including the Convention on the physical protection of nuclear material and nuclear facilities, as appropriate.

(23) ~~Regulation (EC) No 300/2008 of the European Parliament and of the Council[27], Regulation (EC) No 725/2004 of the European Parliament and of the Council[28] and Directive 2005/65/EC of the European Parliament and of the Council[29] 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, when implementing resilience measures under this Directive, critical entities may consider referring to non-binding guidelines and good practices documents developed under sectorial workstreams, such as the EU Rail Passenger Security Platform[30].~~

Other acts of national or Union law may require critical entities to establish resilience measures equivalent to those under Article 11. Member States may choose to recognise equivalence, in whole or in part, between these measures and those referred to in Article 11, or to ensure that critical entities describe those measures in the resilience plan or equivalent document or documents.

---

27 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).

28 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.).

29 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).

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

(24) The risk of employees **or contractors** of critical entities misusing ~~for instance~~ their access rights within the entity's organisation to harm and cause damage is of increasing concern. That risk **may substantiate a need to make provision for a specific procedure for performing background checks for persons designated to undertake sensitive roles or access certain spaces within the critical entities** ~~is exacerbated by the growing phenomenon of radicalisation leading to violent extremism and terrorism~~. It is therefore necessary to enable **Member States, where appropriate, to allow** critical entities to request background checks on **clearly defined categories of** persons ~~falling within specific categories of its personnel~~ and to ensure that those requests are assessed ~~expeditiously by the relevant authorities,~~ in accordance with ~~the applicable rules of Union and national law, including on the protection of personal data~~ **criteria set out in national legislation and procedures**. **Such background checks should, where relevant and applicable, draw upon information obtained from the European Criminal Records Information System (ECRIS)[31] and can also, where relevant and applicable, draw upon the Second Generation Schengen Information System (SIS II)[32], intelligence as well as any other objective information available that may be necessary to determine to suitability of the person concerned to work in the position in relation to which the critical entity has requested a background check.**

---

31 **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**

32 **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) Critical entities should notify, as soon as reasonably possible under the given circumstances, Member States' competent authorities of incidents that significantly disrupt or have the potential to significantly disrupt ~~their operations~~ **the provision of essential services**. The notification should allow the competent authorities to respond to the incidents rapidly and adequately and to have a comprehensive overview of the overall risks that critical entities face. For that purpose, a procedure should be established for the notification of certain incidents and parameters should be provided for to determine when the actual or potential disruption is significant and the incidents should thus be notified. Given the potential cross-border impacts of such disruptions, a procedure should be established for Member States to inform other affected Member States via single points of contacts.

(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 because they provide essential services to ~~a large number of Member States~~ **or in more than one third of Member States**, and therefore **could benefit from specific support at Union level.** ~~require specific oversight at Union level.~~ Rules on ~~the specific oversight~~ **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 of the Commission,** ~~Where any Member State considers that~~ where additional information is necessary to be able to advise a critical entity in meeting its obligations ~~under Chapter III~~ or to assess the compliance of a critical entity of particular European significance with those obligations, in agreement with the Member State where the ~~infrastructure of that~~ entity is located, the Commission should **be enabled 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.

(28) In order to support the Commission and facilitate ~~strategic~~ cooperation **among Member States** and the exchange of information, including best practices, on issues relating to this Directive, a Critical Entities Resilience Group, ~~which is a~~ **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 members holding the appropriate security clearance**. 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.**

(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. **The financial resources for these supporting activities should be provided in line with the agreed allocations in the Multiannual Financial Framework and should be covered in particular from the available envelope foreseen under the Internal Security Fund for the period 2021-2027.**

(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 ~~assess the cybersecurity of those entities~~ **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**. Those competent authorities should cooperate and exchange information for that purpose.

~~(31) In order to take into account new risks, technological developments or specificities of one or more of the sectors, the power to adopt acts in accordance with Article 290 Treaty on the Functioning of the European Union should be delegated to the Commission to supplement the resilience measures critical entities are to take by further specifying some or all of those measures. 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[33]. 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.~~

(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[34].

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

[34] 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).

(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.

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

HAVE ADOPTED THIS DIRECTIVE:

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 ~~certain~~ **specific** measures aimed at ensuring the 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 entities to be treated as equivalent~~ ~~in certain respects~~ and to ~~enable~~ **support** them to meet their obligations;

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

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

(d) ~~and~~ **establishes** ~~specific~~ **rules for** ~~oversight~~ **the identification** of critical entities ~~considered to be~~ of particular European significance **and advisory missions thereto**.

(e) establishes common procedures for cooperation and reporting for the application of the provisions of this Directive.

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.

3. Where provisions of sector-specific acts of Union law require critical entities to take measures ~~as set out in Chapter III~~, and where those requirements are **recognised 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 ~~protect~~ **respect** the s**ecurity of Member States as well as** the security and commercial interests of critical entities.

5. 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.

This Directive does not apply to:

a. entities that fall outside the scope of Union law and, in any event, entities that mainly carry out activities in the areas of defence, national security, public security or law enforcement, regardless of which entity is carrying out those activities and whether it is a public entity or a private entity;

b. entities that carry out activities in the areas of the judiciary, parliaments, or central banks;

c. activities of entities which fall outside the scope of Union law and, in any event, all activities concerning national security or defence, regardless of which entity is carrying out those activities and whether it is a public entity or a private entity.

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.

6. This Directive is without prejudice to Union law on the protection of personal data, in particular Regulation (EU) 2016/679[35] and Directive 2002/58/EC.[36]

---

35 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

36 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 ~~of a type~~ **belonging to the categories** referred to in **the third column of the table in** the Annex, ~~which~~ **and** has been identified as such by a Member State in accordance with Article 5;

(2) "resilience" means **a critical entity's** ~~the~~ ability to prevent, **protect against, respond to,** resist, mitigate, absorb, accommodate ~~to~~ and recover from an incident ~~that disrupts or has the potential to disrupt the operations of a critical entity~~;

(3) "incident" means any event having the potential to **significantly** disrupt, or that disrupts, the ~~operations of the critical entity~~ **provision of an essential service**;

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

(5) "essential service" means a service which is ~~essential~~ **indispensable** for the maintenance of vital societal functions or economic activities;

~~(6) "risk" means any circumstance or event having a potential adverse effect on the resilience of critical entities;~~

(7) "risk assessment" means ~~a methodology~~ **the overall process undertaken by the national competent authorities pursuant to Article 4, or by the critical entities pursuant to Article 10, in order** to determine the nature and extent of **relevant threats, vulnerabilities and** ~~a~~ risk**s** ~~by analysing potential threats and hazards and evaluating existing conditions of vulnerability~~ that could ~~disrupt the operations of the critical entity~~ **lead to an incident**.

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. Each Member State shall adopt by [three years after entry into force of this Directive] a strategy for ~~reinforcing~~ **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** a national risk assessment, the identification **process** of critical entities ~~and of entities equivalent to critical entities~~, and the measures to support critical entities taken in accordance with this Chapter;

(d) a policy framework for ~~enhanced~~ 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 cyber threats~~ and the exercise of supervisory tasks.

The strategy shall be updated ~~where~~ **when** necessary and at least every four years.

3. Member States shall communicate **the relevant aspects of** their strategies, **including of elements referred to in paragraph 2,** and any updates **thereof** ~~of their strategies~~, to the Commission within three months from their adoption.

Article 4

Risk assessment by Member States

1. Competent authorities designated pursuant to Article 8 shall establish a list of essential services in the sectors referred to in the Annex. They shall carry out by [three years after entry into force of this Directive], and subsequently where necessary, and at least every four years, ~~an assessment of all relevant risks that may affect the provision of those essential services,~~ **a risk assessment** with a view to identifying critical entities in accordance with Article 5~~(1),~~ and assisting those critical entities to take measures pursuant to Article 11.

The risk assessment shall account for ~~all~~ relevant natural and man-made risks, including 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[37].

In carrying out the risk assessment, Member States shall take into account ~~as a minimum~~ **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[38];

(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[39]**,** ~~and~~ Regulation (EU) 2017/1938 of the European Parliament and of the Council[40]**, Directive 2012/18/EU of the European Parliament and of the Council[41] and Directive 2007/60/EC of the European Parliament and of the Council[42]**;

---

37 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).

38 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).

39 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).

40 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).

41 **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).**

42 **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).**

(c) any **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;

(d) any **relevant** 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 to the critical entities that they identified in accordance with Article 5**. The information provided to critical entities shall** ~~in order to~~ assist ~~those critical entities~~ **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 ~~data on~~ the types of risks identified and the **summarised** outcomes of the risk assessments, ~~per sector and sub-sector referred to in the Annex~~, ~~by~~ **within** [~~three years after entry into force of this Directive~~ **three months after carrying out the risk assessment**] and subsequently where necessary and at least every four years.

5. The Commission ~~may~~ **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 [~~three years and three months~~ **four years** after entry into force of this Directive] Member States shall identify for ~~each~~ sector**s** and subsector**s** referred to in the Annex~~, other than points 3, 4 and 8 thereof~~, the critical entities.

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 apply **all** ~~the~~ following criteria:

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

   (b) ~~(the provision of that service depends on~~ **the entity and its critical** infrastructure **are** located ~~in~~ **on** the **territory of the** Member State **performing the identification**; and

   (c) an incident would have significant disruptive effects on the provision of ~~the~~ **these essential** service**s** or of other essential services in the sectors referred to in the Annex ~~that depend on the service~~ **pursuant to Article 6(1)**.

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~~ing~~ those critical entities ~~them~~ of their obligations pursuant to Chapters ~~II~~ **III** and ~~III~~ **IV** and the date from which ~~the~~ **these** provisions ~~of those Chapters~~ apply to them**, without prejudice to Article 7**.

For the critical entities concerned, ~~the provisions of this Chapter shall apply from the date of the notification and~~ the provisions of ~~Chapter~~ **Chapters** III **and IV** shall apply from ~~six~~ **twelve** months after that date**, except for the provisions of Article 14(2)(a) which shall apply from the date of the notification**.

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

~~5. Following the notification referred in paragraph 3, Member States shall ensure that critical entities provide information to their competent authorities designated pursuant to Article 8 of this Directive on whether they have been identified as a critical entity in one or more other Member States. Where an entity has been identified as critical by two or more Member States, these Member States shall engage in consultation with each other with a view to reduce the burden on the critical entity in regard to the obligations pursuant to Chapter III.~~

6. ~~For the purposes of Chapter IV, Member States shall ensure that critical entities, following the notification referred in paragraph 3, provide information to their competent authorities designated pursuant to Article 8 of this Directive on whether they provide essential services to or in more than one third of Member States. Where that is so, the Member State concerned shall notify, without undue delay, to the Commission the identity of those critical entities.~~

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 ~~, 5 and 6~~ 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 that they are no longer subject to the obligations pursuant to Chapter III as from the reception of that information.

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 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**,** ~~and~~ 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;

   (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 service.

2. Member States shall submit to the Commission ~~by~~ **within** [~~three years and~~ three months ~~after~~ **of the** ~~the entry into force of this Directive~~ **identification of the critical entities**] the following information:

   (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 the service or services referred to in Article 4(1) that each entity provides~~;

(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 ~~may~~ **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

*~~Entities equivalent to~~ ~~c~~**C**ritical entities ~~under this Chapter~~ in the banking, financial market infrastructure and digital infrastructure sectors*

~~1. As regards the sectors referred to in points 3, 4 and 8 of the Annex, Member States shall, by [three years and three months after entry into force of this Directive], identify the entities that shall be treated as equivalent to critical entities for the purposes of this Chapter. They shall apply the provisions of Articles 3, 4, 5(1) to (4) and (7), and 9 in respect of those entities.~~

~~2. In respect of the entities in the sectors referred to in points 3 and 4 of the Annex identified pursuant to paragraph 1, Member States shall ensure that, for the purposes of the application of Article 8(1), the authorities designated as competent authorities are the competent authorities designated pursuant to Article 41 of [DORA Regulation].~~

~~3. Member States shall ensure that the entities referred to in paragraph 1 are, without undue delay, notified of their identification as entities referred to in this Article.~~

Member States shall ensure that the provisions of Article 9a and Chapters III to VI shall not apply in respect of designated critical entities in the sectors referred to in points 3, 4 and 8 of the table in the Annex.

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, where appropriate, be the competent authorities designated pursuant to Article 41 of [DORA Regulation].
   In respect of critical entities referred to in point 8 of the table in the Annex, the designated competent authorities shall, where appropriate, be the competent authorities designated pursuant to Article 8 of [NIS 2 Directive].

   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~~, within the competent authority,~~ designate ~~a~~ **one national** single point of contact to exercise a liaison function to ensure cross-border cooperation with ~~competent authorities~~ **the single points of contact** of other Member States and with the Critical Entities Resilience Group referred to in Article 16 ('single point of contact').

3. By [~~three~~ **seven** years ~~and six months~~ after entry into force of this Directive], and every **two** ~~year~~ **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).

The Commisison shall, in cooperation with the Critical Entities Resilience Group, develop a voluntary common reporting template for the summary report referred to in the subpargaraph above.

4. Each Member State shall ensure that the competent authority~~, including~~ **and** the single point of contact ~~designated therein, has~~ **have** the powers and the adequate financial, human and technical resources to carry out, in an effective and efficient manner, the tasks assigned to ~~it~~ **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, ~~in particular~~ **including** those in charge of civil protection, law enforcement and protection of personal data, as well as **critical entities and** ~~with~~ relevant interested parties~~, including critical entities~~.

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 ~~cyber~~ incidents **and non-cyber risks, threats and incidents** affecting critical entities, as well as ~~the~~ **relevant** measures taken by competent authorities designated under [the NIS 2 Directive] **and this Directive** ~~relevant for critical entities~~.

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 ~~precise~~ 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.

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 ~~establish information sharing tools to support~~ **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 ~~six~~ **twelve** 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 operations~~ **the provision of essential services**.

The risk assessment **of the critical entities** shall account for ~~all~~ relevant risks referred to in Article 4(1) which could lead to ~~the disruption of the provision of essential services~~ **an incident**. It shall take into account ~~any dependency~~ **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**.**~~, and the impact that a disruption of the provision of essential services in one or more of those sectors may have on the essential service provided by the critical entity.~~ **Member States may recognise equivalence, in whole or in part, between exisiting risk assessments of critical entities in as far as they address the risks and dependencies referred to in 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 outcomes of the risk assessments referred to in Articles 4 and 10**, including measures necessary to:

   (a) prevent incidents from occurring, ~~including through~~ **duly taking into account** disaster risk reduction and climate adaptation measures;

(b) ensure adequate physical protection **of the premises and the critical infrastructure** ~~sensitive areas, facilities and other infrastructure, including~~ **duly taking into account 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~~, including~~ **duly taking into account** the implementation of risk and crisis management procedures and protocols and alert routines;

(d) recover from incidents, ~~including~~ **duly taking into account** business continuity measures and the identification of alternative supply chains;

(e) ensure adequate employee security management, ~~including~~ **duly taking into account measures such as** ~~by~~ setting out categories of personnel exercising critical functions, establishing access rights to ~~sensitive areas, facilities and other~~ **premises, critical** infrastructure, and ~~to~~ sensitive information**,** as well as ~~identifying~~ **designating the** ~~specific~~ categories of ~~personnel~~ **persons and setting up vetting procedures** in ~~view of~~ **accordance with** Article 12;

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

2. Member States shall ensure that critical entities have in place and apply a resilience plan or equivalent document or documents, describing ~~in detail~~ the measures pursuant to paragraph 1. Where critical entities have taken measures pursuant to obligations contained in other acts of Union, **national or international** law ~~that are also relevant for the measures referred to in paragraph 1,~~**. Member States may recognise equivalence, in whole or in part, between the measures referred to in paragraph 1 and these measures or ensure that critical entities** ~~they shall also~~ describe those measures in the resilience plan or equivalent document or documents.

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~~(4),~~ (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 is empowered to adopt delegated acts in accordance with Article 21 supplementing paragraph 1 by establishing detailed rules specifying some or all of the measures to be taken pursuant to that paragraph. It shall adopt those delegated acts in as far as necessary for the effective and consistent application of that paragraph in accordance with the objectives of this Directive, having regard to any relevant developments in risks, technology or the provision of the services concerned as well as to any specificities relating to particular sectors and types of entities.~~

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 **may, where appropriate,** ~~shall~~ ensure that critical entities ~~may~~ **are permitted to** submit requests for background checks on persons who:

a) **perform sensitive or designated roles in or for the critical entity;**

b) **are mandated to use or maintain – directly or remotely - its premises including in connection with the security of persons, goods or information;** ~~fall within certain specific categories of their personnel~~, ~~including~~

c) ~~persons~~ **are** being considered for recruitment to positions ~~falling~~ ~~within those categories~~ **involving the roles mentioned under points a) and b).**

~~, and that those~~ **Those** requests ~~are~~ **shall be** assessed **within a reasonable timeframe** ~~expeditiously by the authorities competent to carry out such background checks.~~ **and processed in accordance with national legislation and procedures.**

2. ~~In accordance with applicable Union and national law, including Regulation (EU) 2016/679/EU of the European Parliament and of the Council [43], a background check as referred to in paragraph 1 shall~~

~~(a) establish the person's identity on the basis of documentary evidence;~~

~~(b) cover any criminal records of at least the preceding five years, and for a maximum of ten years, on crimes relevant for recruitment on a specific position, in the Member State or Member States of nationality of the person and in any of the Member States or third countries of residence during that period of time;~~

~~(c) cover previous employments, education and any gaps in education or employment in the person's resume during at least the preceding five years and for a maximum of ten years.~~

~~As regards point (b) of the first subparagraph, Member States shall ensure that their authorities competent to carry out background checks~~ **Member States shall, for the purpose of** obtain**ing** the information on criminal records from other Member States**, use the European Criminal Records Information System** ~~through~~ **(**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[44]. 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**.

---

43 OJ L 119, 4.5.2016, p. 1.

44 OJ L 135, 22.5.2019, p. 1.

~~3. In accordance with applicable Union and national law, including Regulation (EU) 2016/679, each Member State shall ensure that a background check as referred to in paragraph 1 may also be extended, on the basis of a duly justified request of the critical entity, to draw upon intelligence and any other objective information available that may be necessary to determining the suitability of the person concerned to work in the position in relation to which the critical entity has requested an extended background check.~~

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 ~~their operations~~ **the provision of essential services**. ~~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.~~ **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.

2. ~~In order to determine the significance of the disruption or the potential disruption to the critical entity's operations resulting from an incident, the following parameters shall, in particular, be taken into account:~~

~~(a) the number of users affected by the disruption or potential disruption;~~

~~(b) the duration of the disruption or anticipated duration of a potential disruption;~~

~~(c) the geographical area affected by the disruption or potential disruption.~~

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 ~~its~~ **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 ~~that complies with Union law~~, 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 ~~that notified it~~ with relevant ~~information regarding the~~ follow-up **information** ~~of its notification~~, including information that could support the critical entity's effective response to the incident.

CHAPTER IV

~~SPECIFIC OVERSIGHT OVER~~ CRITICAL ENTITIES OF PARTICULAR EUROPEAN SIGNIFICANCE

Article 14

Identification of *Critical entities of particular European significance*

~~1. Critical entities of particular European significance shall be subject to specific oversight, in accordance with this Chapter.~~

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),** ~~and~~ it provides essential services to or in more than one third of Member States and **it** has been notified ~~as such to the Commission~~ pursuant to ~~Article 5(1) and (6), respectively.~~ **paragraph 3;**

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 more than one third of 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 more than one third of Member States,** ~~The Commission~~ **it** shall ~~without undue delay upon receiving the notification pursuant to Article 5(6),~~ 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.

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

Article 15

~~*Specific oversight*~~ ***Advisory Missions***

1. ~~Upon request of one or more Member States or of the Commission, the Member State where the infrastructure of the critical entity of particular European significance is located shall, together with that entity, inform the Commission and the Critical Entities Resilience Group of the outcome of the risk assessment carried out pursuant to Article 10 and the measures taken in accordance with Article 11.~~

   ~~That Member State shall also inform, without undue delay, the Commission and the Critical Entities Resilience Group of any supervisory or enforcement actions, including any assessments of compliance or orders issued, that its competent authority has undertaken pursuant to Articles 18 and 19 in respect of that entity.~~

   The Member State where a critical entity of particular European significance is located may request the Commission to organise an advisory mission to assess the measures that the entity concerned 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 where the critical entity of particular European significance is located, the Commission shall organise such an advisory mission.

2. ~~Upon request of one or more Member States, or at its own initiative, and in agreement with the Member State where the infrastructure of the critical entity of particular European significance is located, the Commission shall organise an advisory mission to assess the measures that that entity put in place to meet its obligations pursuant to Chapter III. Where needed, the advisory missions may request specific expertise in the area of disaster risk management through the Emergency Response Coordination Centre.~~

Upon reasoned request of one or more Member States to or in which the essential service is provided, or the Commission, the Member State where the critical entity of particular European significance is located shall provide:

a. a summarised outcome of the risk assessment carried out pursuant to Article 10;

b. a summary of measures taken in accordance with Article 11;

c. 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 Critical Entities Resilience Group and the critical entity of particular European significance concerned~~**, 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 the entity concerned** within a period of three months after the conclusion of the advisory mission.

~~The Critical Entities Resilience Group~~ **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 ~~views~~ **opinion** to the Member State where ~~the infrastructure of~~ that entity is located, ~~the Critical Entities Resilience Group~~ **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 the competent authority and the critical entity concerned** take due account of ~~those views~~ **that opinion** and provide information to the Commission and ~~the Critical Entities Resilience Group~~ **the Member States to or in which the essential service is provided** on ~~any~~ measures it has taken pursuant to ~~the communication~~ **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 where the critical entity is located**, select and appoint the members of each advisory mission according to their professional capacity and ensuring **where possible** a geographically balanced representation ~~among~~ **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 where ~~the infrastructure of the critical entity or~~ the critical entity of European significance concerned is located.

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 commerical 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 ~~all~~ information, systems and facilities relating to the provision of its essential services necessary for ~~the performance of its tasks~~ **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 ~~that infrastructure~~ **the critical entity of particular European significance** is located**, 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.

9. The Commission shall inform the Critical Entities Resilience Group whenever an advisory mission is organised. The Member State where the critical entity of particular European significance is located and the Commission shall also inform the Critical Entities Resilience Group of the summary report 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 ~~strategic~~ 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 ~~representatives of interested parties~~ **other stakeholders** to participate in its work.

   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) ~~evaluating~~ **analysing** the strategies on the resilience of critical entities referred to in Article 3 ~~and identifying~~ **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 dependencies and regarding risks and incidents**,** ~~;~~ **as well as with regard to the national approach to implementing the equivalence regime;**

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

(e) ~~examining~~ **analysing**~~, on an annual basis,~~ the summary reports referred to in Article 8(3);

(f) exchanging best practices ~~on the exchange of information~~ related to the notification of incidents referred to in Article 13;

(g) ~~analyse and provide advice on~~ **discuss** the **summary** reports of advisory missions **and lessons-learned** in accordance with Article 15(~~3~~**9**);

(h) exchanging information and best practices on 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 promote ~~strategic~~ cooperation and **facilitate** exchange of information.

6. The Commission ~~may~~ **shall** 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 [three years and ~~six~~ **nine** months 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**.**~~, in particular by~~ ~~preparing~~ **The Commission shall prepare** a Union-level overview of cross-border and cross-sectoral risks to the provision of essential services, ~~organising~~ **organise** the advisory missions referred to in Articles 11(3) and 15~~(3)~~ and ~~facilitating~~ **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.

3. The Commission shall make financial sources available to Member States for enhancing the resilience of their 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 ~~its~~ **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 and operations,** 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 ~~assess the cybersecurity of such entity,~~ **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 [two years 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 11(4) 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 11(4) 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 11(4) 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~~ **six years** 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 the Member States have 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 ~~scope of the~~ **Annex of the** Directive should be ~~extended to cover other sectors or subsectors~~ **modified**. The first report shall be submitted by [~~six years~~ **7 years and 6 months** after the entry into force of this Directive] ~~and shall assess in particular whether the scope of the Directive should be extended to include the food production, processing and distribution sector~~.

Article 23

Repeal of Directive 2008/114/EC

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

Article 24

Transposition

1. Member States shall adopt and publish, by [~~18 months~~ **two years** 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 [two years 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 ~~types~~ **categories** of entities

Sector**s**	Subsector**s**	~~Type~~ **Categories** of entit~~y~~**ies**
1. Energy	(a) Electricity	— Electricity undertakings referred to in point (57) of Article 2 of Directive (EU) 2019/944[45], 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[46]

[45] 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

[46] 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).

		— 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[47] 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[48]

[47] 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).

[48] 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).

	(d) Gas	— Supply undertakings referred to in point (8) of Article 2 of Directive (EU) 2009/73/EC[49]
		— 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

[49] 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).

	(e) Hydrogen	— Operators of hydrogen production, storage and transmission
2. Transport	(a) Air	— Air carriers referred to in point (4) of Article 3 of Regulation (EC) No 300/2008[50] **used for commercial purposes**
		— Airport managing bodies referred to in point (2) of Article 2 of Directive 2009/12/EC[51] , 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[52], 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[53]

50 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).

51 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).

52 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).

53 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).

	(b) Rail	— Infrastructure managers referred to in point (2) of Article 3 of Directive 2012/34/EU[54]
		— Railway undertakings referred to in point (1) of Article 3 of Directive 2012/34/EU, ~~including~~ **and** operators of service facilities referred to in point (12) of Article 3 of Directive 2012/34/EU

[54] 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).

	(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[55], not including the individual vessels operated by those companies
		— Managing bodies of ports referred to in point (1) of Article 3 of Directive 2005/65/EC[56], 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[57] of the European Parliament and of the Council

[55] 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).

[56] 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).

[57] 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).

	(d) Road	— Road authorities referred to in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962[58] 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[59]
3. Banking **- solely for the purposes of Articles 1-9 of this Directive**		Credit institutions referred to in point (1) of Article 4 of Regulation (EU) No 575/2013[60]

[58] 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).

[59] 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).

[60] 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).

4. Financial market infrastructures **- solely for the purposes of Articles 1-9 of this Directive**		— Operators of trading venues referred to in point (24) of Article 4 of Directive 2014/65/EU[61]
		— Central counterparties (CCPs) referred to in point (1) of Article 2 of Regulation (EU) No 648/2012[62]
5. Health		— Healthcare providers referred to in point (g) of Article 3 of Directive 2011/24/EU[63]
		— EU reference laboratories referred to in Article 15 of Regulation [XX] on serious cross borders threats to health[64]

61 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).

62 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).

63 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).

64 [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].

		— Entities carrying out research and development activities of medicinal products referred to in Article 1 point 2 of Directive 2001/83/EC[65]
		— 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 20 of Regulation XXXX[66]

[65] 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).

[66] [Regulation on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal produces and medical devices COM(2020) 725 final] reference once the proposal is updated].

6. Drinking water		Suppliers and distributors of water intended for human consumption referred to in point (1)(a) of Article 2 of Council Directive 98/83/EC[67] 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 ~~which are not considered essential or important services~~
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[68]**, but excluding undertakings for whom colecting, disposing or treating of urban, domestic and industrial waste water is only a non-essential part of their general activity**

[67] Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption (OJ L 330, 5.12.1998, p. 32).

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

8. Digital infrastructure **- solely for the purposes of Articles 1-9 of this Directive**		— 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[69]
		— Providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972[70] 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

[69] 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).

[70] 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).

~~9. Public administration~~		~~— Public administration entities, [referred to in point (X) of Article 4 of NIS 2 Directive], of central governments~~
		~~— Public administration entities, [referred to in point (X) of Article 4 of NIS 2 Directive], of NUTS level 1 regions listed in Annex I to Regulation (EC) No 1059/2003~~[71]
		~~— Public administration entities, [referred to in point (X) of Article 4 of NIS 2 Directive], of NUTS level 2 regions listed in Annex I to Regulation (EC) No 1059/2003~~

[71] Regulation (EC) No 1059/2003 of the European Parliament and of the Council of 26 May 2003 on the establishment of a common classification of territorial units for statistics (NUTS) (OJ L 154, 21.6.2003, p. 1).

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

89