DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on the resilience of critical entities and repealing Council Directive 2008/114/EC

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

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

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

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

Whereas:

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

(2) Council Directive 2008/114/EC ([4]) provides for a procedure for designating European critical infrastructure in the energy and transport sectors the disruption or destruction of which would have a significant cross-border impact on at least two Member States. That Directive focuses exclusively on the protection of such infrastructure. However, the evaluation of Directive 2008/114/EC conducted in 2019 found that, due to the increasingly interconnected and cross-border nature of operations using critical infrastructure, protective measures relating to individual assets alone are insufficient to prevent all disruptions from taking place. Therefore, it is necessary to shift the approach towards ensuring that risks are better accounted for, that the role and duties of critical entities as providers of services essential to the functioning of the internal market are better defined and coherent, and that Union rules are adopted

([1]) OJ C 286, 16.7.2021, p. 170.
([2]) OJ C 440, 29.10.2021, p. 99.
([3]) Position of the European Parliament of 22 November 2022 (not yet published in the Official Journal) and Council decision of 8 December 2022.
([4]) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75).

to enhance the resilience of critical entities. Critical entities should be in a position to reinforce their ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from incidents that have the potential to disrupt the provision of essential services.

(3) While a number of measures at Union level, such as the European Programme for Critical Infrastructure Protection, and at national level aim to support the protection of critical infrastructure in the Union, more should be done to better equip the entities operating such infrastructure to address the risks to their operations that could result in the disruption of the provision of essential services. More should also be done to better equip such entities because there is a dynamic threat landscape, which includes evolving hybrid and terrorist threats, and growing interdependencies between infrastructure and sectors. Moreover, there is an increased physical risk due to natural disasters and climate change, which intensifies the frequency and scale of extreme weather events and brings long-term changes in average climate conditions that can reduce the capacity, efficiency and lifespan of certain infrastructure types if climate adaptation measures are not in place. In addition, the internal market is characterised by fragmentation in respect of the identification of critical entities because relevant sectors and categories of entities are not recognised consistently as critical in all Member States. This Directive should therefore achieve a solid level of harmonisation in terms of the sectors and categories of entities falling within its scope.

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

(5) The growing interdependencies between infrastructure and sectors are the result of an increasingly cross-border and interdependent network of service provision using key infrastructure across the Union in the energy, transport, banking, drinking water, waste water, production, processing and distribution of food, health, space, financial market infrastructure and digital infrastructure sectors and in certain aspects of the public administration sector. The space sector falls within the scope of this Directive with respect to the provision of certain services that depend on ground-based infrastructure owned, managed and operated either by Member States or by private parties; consequently, infrastructure owned, managed or operated by or on behalf of the Union as part of its space programme does not fall within the scope of this Directive.

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

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

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

(8) In order to achieve a high level of resilience, Member States should identify critical entities that will be subject to specific requirements and supervision and that will be provided with particular support and guidance in the face of all relevant risks.

(9) Given the importance of cybersecurity for the resilience of critical entities and in the interests of consistency, a coherent approach should be ensured, wherever possible, between this Directive and Directive (EU) 2022/2555 of the European Parliament and of the Council ([5]). In light of the higher frequency and particular characteristics of cyber risks, Directive (EU) 2022/2555 imposes comprehensive requirements on a large set of entities to ensure their cybersecurity. Given that cybersecurity is addressed sufficiently in Directive (EU) 2022/2555, the matters covered by that Directive should be excluded from the scope of this Directive, without prejudice to the particular regime for entities in the digital infrastructure sector.

(10) Where provisions of sector-specific Union legal acts require critical entities to take measures to enhance their resilience, and where those requirements are recognised by Member States as at least equivalent to the corresponding obligations laid down in this Directive, the relevant provisions of this Directive should not apply, so as to avoid duplication and unnecessary burden. In that case, the relevant provisions of such Union legal acts should apply. Where the relevant provisions of this Directive do not apply, the provisions on supervision and enforcement laid down in this Directive should not apply either.

(11) This Directive does not affect the competence of Member States and their authorities in terms of administrative autonomy or their responsibility for safeguarding national security and defence or their power to safeguard other essential State functions, in particular concerning public security, territorial integrity and the maintenance of law and order. The exclusion of public administration entities from the scope of this Directive should apply to entities whose activities are predominantly carried out in the areas of national security, public security, defence or law enforcement, including the investigation, detection and prosecution of criminal offences. However, public administration entities whose activities are only marginally related to those areas should fall within the scope of this Directive. For the purposes of this Directive, entities with regulatory competences are not considered to be carrying out activities in the area of law enforcement and are therefore not excluded on that ground from the scope of this Directive. Public administration entities that are jointly established with a third country in accordance with an international agreement are excluded from the scope of this Directive. This Directive does not apply to Member States' diplomatic and consular missions in third countries.

([5]) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (see page 80 of this Official Journal).

Certain critical entities carry out activities in the areas of national security, public security, defence or law enforcement, including the investigation, detection and prosecution of criminal offences, or provide services exclusively to public administration entities that carry out activities predominantly in those areas. In light of the Member States' responsibility for safeguarding national security and defence, Member States should be able to decide that the obligations on critical entities laid down in this Directive do not apply, in whole or in part, to those critical entities if the services they provide or the activities they perform are predominantly related to the areas of national security, public security, defence or law enforcement, including the investigation, detection and prosecution of criminal offences. Critical entities whose services or activities are only marginally related to those areas should fall within the scope of this Directive. No Member State should be required to supply information the disclosure of which would be contrary to the essential interests of its national security. Union or national rules for the protection of classified information and non-disclosure agreements are of relevance.

(12) In order not to jeopardise national security or the security and commercial interests of critical entities, sensitive information should be accessed, exchanged and handled prudently and with particular attention to the transmission channels and storage capacities used.

(13) With a view to ensuring a comprehensive approach to the resilience of critical entities, each Member State should have in place a strategy for enhancing the resilience of critical entities (the 'strategy'). The strategy should set out the strategic objectives and policy measures to be implemented. In the interests of coherence and efficiency, the strategy should be designed to seamlessly integrate existing policies, building, wherever possible, upon relevant existing national and sectoral strategies, plans or similar documents. In order to achieve a comprehensive approach, Member States should ensure that their strategies provide for a policy framework for enhanced coordination between the competent authorities under this Directive and the competent authorities under Directive (EU) 2022/2555 in the context of information sharing on cybersecurity risks, cyber threats and cyber incidents and non-cyber risks, threats and incidents and in the context of the exercise of supervisory tasks. When putting in place their strategies, Member States should take due account of the hybrid nature of threats to critical entities.

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

(15) The actions of Member States to identify and help ensure the resilience of critical entities should follow a risk-based approach that focuses on the entities most relevant for the performance of vital societal functions or economic activities. In order to ensure such a targeted approach, each Member State should carry out, within a harmonised framework, an assessment of the relevant natural and man-made risks, including those of a cross-sectoral or cross-border nature, that could affect the provision of essential services, including accidents, natural disasters, public health emergencies such as pandemics and hybrid threats or other antagonistic threats, including terrorist offences, criminal infiltration and sabotage ('Member State risk assessment'). When carrying out Member State risk assessments, Member States should take into account other general or sector-specific risk assessments carried out pursuant to other Union legal acts and should consider the extent to which sectors depend on one another, including on sectors in other Member States and third countries. The outcome of Member State risk assessments should be used for the purposes of identifying critical entities and assisting those entities in meeting their resilience requirements. This Directive applies only to Member States and critical entities that operate within the Union.

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

(16) In order to ensure that all relevant entities are subject to the resilience requirements of this Directive and to reduce divergences in that respect, it is important to lay down harmonised rules allowing for a consistent identification of critical entities across the Union, while also allowing Member States to adequately reflect the role and importance of those entities at national level. When applying the criteria laid down in this Directive, each Member State should identify entities that provide one or more essential services and that operate and have critical infrastructure located on its territory. An entity should be considered to operate on the territory of a Member State in which it carries out activities necessary for the essential service or services in question and in which that entity's critical infrastructure, which is used to provide that service or those services, is located. Where no entity meets those criteria in a Member State, that Member State should be under no obligation to identify a critical entity in the corresponding sector or subsector. In the interests of effectiveness, efficiency, consistency and legal certainty, appropriate rules should be established as regards notifying entities that they have been identified as critical entities.

(17) Member States should submit to the Commission, in a manner that fulfils the objectives of this Directive, a list of essential services, the number of critical entities identified for each of the sectors and subsectors set out in the Annex and for the essential service or services that each entity provides and, if applied, thresholds. It should be possible to present thresholds as such or in aggregated form, meaning that the information can be averaged by geographic area, by year, by sector, by subsector or by other means, and can include information on the range of the indicators provided.

(18) Criteria should be established to determine the significance of a disruptive effect produced by an incident. Those criteria should build on the criteria set out in Directive (EU) 2016/1148 of the European Parliament and of the Council ([6]) in order to capitalise on the efforts carried out by Member States to identify operators of essential services as defined in that Directive and the experience gained in that regard. Major crises, such as the COVID-19 pandemic, have shown the importance of ensuring the security of the supply chain and have demonstrated how its disruption can have a negative economic and societal impact across a large number of sectors and across borders. Therefore, Member States should also consider effects on the supply chain, to the extent possible, when determining the extent to which other sectors and subsectors depend on the essential service provided by a critical entity.

(19) In accordance with applicable Union and national law, including Regulation (EU) 2019/452 of the European Parliament and of the Council ([7]), which establishes a framework for the screening of foreign direct investments in the Union, the potential threat posed by foreign ownership of critical infrastructure within the Union is to be acknowledged because services, the economy and the free movement and safety of Union citizens depend on the proper functioning of critical infrastructure.

(20) Directive (EU) 2022/2555 requires entities belonging to the digital infrastructure sector, which might be identified as critical entities under this Directive, to take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems and to notify significant incidents and cyber threats. Since threats to the security of network and information systems can have different origins, Directive (EU) 2022/2555 applies an all-hazards approach that includes the resilience of network and information systems, as well as the physical components and environment of those systems.

([6]) 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).

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

Given that the requirements laid down in Directive (EU) 2022/2555 in that regard are at least equivalent to the corresponding obligations laid down in this Directive, the obligations laid down in Article 11 and Chapters III, IV and VI of this Directive should not apply to entities belonging to the digital infrastructure sector in order to avoid duplication and unnecessary administrative burden. However, considering the importance of the services provided by entities belonging to the digital infrastructure sector to critical entities belonging to all other sectors, Member States should identify, based on the criteria and using the procedure provided for in this Directive, entities belonging to the digital infrastructure sector as critical entities. Consequently, the strategies, the Member State risk assessments and the support measures set out in Chapter II of this Directive should apply. Member States should be able to adopt or maintain provisions of national law to achieve a higher level of resilience for those critical entities, provided that those provisions are consistent with applicable Union law.

(21) Union financial services law establishes comprehensive requirements on financial entities to manage all risks they face, including operational risks, and to ensure business continuity. Such law includes Regulations (EU) No 648/2012 ([8]), (EU) No 575/2013 ([9]) and (EU) No 600/2014 ([10]) of the European Parliament and of the Council and Directives 2013/36/EU ([11]) and 2014/65/EU ([12]) of the European Parliament and of the Council. That legal framework is complemented by Regulation (EU) 2022/2554 of the European Parliament and of the Council ([13]), which lays down requirements applicable to financial entities to manage Information and Communication Technology (ICT) risks, including concerning the protection of physical ICT infrastructure. Since the resilience of those entities is therefore comprehensively covered, Article 11 and Chapters III, IV and VI of this Directive should not apply to those entities in order to avoid duplication and unnecessary administrative burden.

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

(22) Member States should designate or establish 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 light of the differences in national governance structures, in order to safeguard existing sectoral arrangements or Union supervisory and regulatory bodies, and in order to avoid duplication, Member States should be able to designate or establish more than one competent authority. Where Member States designate or establish more than one competent authority, they should 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, at both Union and national level.

([8]) 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).

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

([10]) 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).

([11]) 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).

([12]) 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).

([13]) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (see page 1 of this Official Journal).

(23) 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 the requirements of sector-specific Union legal acts, designate one single point of contact responsible for coordinating issues related to the resilience of critical entities and cross-border cooperation at Union level ('single point of contact'), where relevant within a competent authority. Each single point of contact should liaise and coordinate communication, where relevant, with the competent authorities of its Member State, with the single points of contact of other Member States and with the Critical Entities Resilience Group.

(24) The competent authorities under this Directive and the competent authorities under Directive (EU) 2022/2555 should cooperate and exchange information in relation to cybersecurity risks, cyber threats and cyber incidents and non-cyber risks, threats and incidents affecting critical entities as well as in relation to relevant measures taken by competent authorities under this Directive and competent authorities under Directive (EU) 2022/2555. It is important that Member States ensure that the requirements provided for in this Directive and in Directive (EU) 2022/2555 are implemented in a complementary manner and that critical entities are not subject to an administrative burden beyond that which is necessary to achieve the objectives of this Directive and that Directive.

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

(26) With the aim of enhancing the resilience of critical entities identified by Member States and in order to reduce the administrative burden on those critical entities, the competent authorities should consult one another, whenever appropriate, for the purpose of ensuring that this Directive is applied in a consistent manner. Those consultations should be entered into at the request of any interested competent authority and should focus on ensuring a convergent approach regarding interlinked 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 that provide essential services to or in other Member States.

(27) 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 purpose of supervising the compliance of critical entities with this Directive.

(28) Critical entities should have a comprehensive understanding of the relevant risks to which they are exposed and a duty to analyse those risks. To that end, they should carry out risk assessments whenever necessary in view of their particular circumstances and the evolution of those risks and, in any event, every four years, in order to assess all relevant risks that could disrupt the provision of their essential services ('critical entity risk assessment'). Where critical entities have carried out other risk assessments or drawn up documents pursuant to obligations laid down in other legal acts that are relevant for their critical entity risk assessment, they should be able to use those assessments and documents to meet the requirements set out in this Directive concerning critical entity risk assessments. A competent authority should be able to declare that an existing risk assessment carried out by a critical entity that addresses the relevant risks and the relevant extent of dependence is compliant, in whole or in part, with the obligations laid down in this Directive.

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

(30) In the interests of effectiveness and accountability, critical entities should describe the measures they take, with a level of detail that sufficiently achieves the aims of effectiveness and accountability, 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. Where a critical entity has already taken technical, security and organisational measures and drawn up documents pursuant to other legal acts that are relevant for resilience-enhancing measures under this Directive, it should be able, in order to avoid duplication, to use those measures and documents to meet the requirements as regards resilience measures under this Directive. In order to avoid duplication, a competent authority should be able to declare existing resilience measures taken by a critical entity that address its obligation to take technical, security and organisational measures pursuant to this Directive as compliant, in whole or in part, with the requirements of this Directive.

(31) Regulations (EC) No 725/2004 ([14]) and (EC) No 300/2008 ([15]) of the European Parliament and of the Council and Directive 2005/65/EC of the European Parliament and of the Council ([16]) 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 under 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 legal acts. Critical entities are also to take into consideration Directive 2008/96/EC of the European Parliament and of the Council ([17]), which introduces a network-wide road assessment to map the risk of accidents and a targeted road safety inspection to identify hazardous conditions, defects and problems that increase the risk of accidents and injuries, based on site visits of existing roads or sections of roads. Ensuring the protection and resilience of critical entities is of the utmost importance for the railway sector and, when implementing resilience measures under this Directive, critical entities are encouraged to refer to non-binding guidelines and good practices documents developed under sectorial workstreams, such as the EU Rail Passenger Security Platform set up by Commission Decision 2018/C 232/03 ([18]).

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

([14]) 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).

([15]) 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).

([16]) 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).

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

([18]) Commission Decision of 29 June 2018 setting up the EU Rail Passenger Security Platform 2018/C 232/03 (OJ C 232, 3.7.2018, p. 10).

Background checks should include a check of the criminal records of the person concerned. Member States should use the European Criminal Records Information System in accordance with the procedures set out in Council Framework Decision 2009/315/JHA ([19]) and, where relevant and applicable, Regulation (EU) 2019/816 of the European Parliament and of the Council ([20]) for the purpose of obtaining information from criminal records held by other Member States. Member States might also, where relevant and applicable, draw on the Second Generation Schengen Information System (SIS II) established by Regulation (EU) 2018/1862 of the European Parliament and of the Council ([21]), intelligence and any other objective information available that might be necessary to determine the suitability of the person concerned to work in the position in relation to which the critical entity has requested a background check.

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

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

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

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

([19]) Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States (OJ L 93, 7.4.2009, p. 23).

([20]) Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 (OJ L 135, 22.5.2019, p. 1).

([21]) 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, 7.12.2018, p. 56).

without prejudice to the need for the Member State in which the advisory mission is conducted and the critical entity concerned to comply with the rules laid down in 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 in order to obtain access to relevant premises or documents and on judicial redress. Specific expertise required for such advisory missions could, where relevant, be requested through the Emergency Response Coordination Centre established by Decision No 1313/2013/EU of the European Parliament and of the Council ([22]).

(37) In order to support the Commission and facilitate cooperation among Member States and the exchange of information, including best practices, on issues relating to this Directive, a Critical Entities Resilience Group should be established as a Commission expert group. Member States should endeavour to ensure that the designated representatives of their competent authorities in the Critical Entities Resilience Group effectively and efficiently cooperate, including by designating representatives who hold security clearance, where appropriate. The Critical Entities Resilience Group should begin to perform its tasks as soon as possible, so as to provide additional means for appropriate cooperation during the transposition period of this Directive. The Critical Entities Resilience Group should interact with other relevant sector-specific expert working groups.

(38) The Critical Entities Resilience Group should cooperate with the Cooperation Group established under Directive (EU) 2022/2555 with a view to supporting a comprehensive framework for cyber and non-cyber resilience of critical entities. The Critical Entities Resilience Group and the Cooperation Group established under Directive (EU) 2022/2555 should engage in a regular dialogue to promote cooperation between the competent authorities under this Directive and the competent authorities under Directive (EU) 2022/2555 and to facilitate the exchange of information, in particular on topics of relevance to both groups.

(39) 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 laid down therein, the Commission should, where it considers it appropriate, support competent authorities and critical entities with the aim of facilitating their compliance with their respective 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, established by Decision No 1313/2013/EU, and the European Reference Network for Critical Infrastructure Protection. In addition, it should inform Member States about resources available at Union level, such as within the Internal Security Fund, established by Regulation (EU) 2021/1149 of the European Parliament and of the Council ([23]), Horizon Europe, established by Regulation (EU) 2021/695 of the European Parliament and of the Council ([24]), or other instruments relevant for the resilience of critical entities.

(40) 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, in particular, the power to conduct inspections and audits, the power to supervise, the power to require critical entities to provide information and evidence relating to the measures they have taken to comply with their obligations and, where necessary, the power to 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 the compliance of the critical entity concerned, taking account of, in particular, the seriousness of the infringement and the economic capacity of the critical entity concerned. More generally, those powers should be accompanied by appropriate and effective safeguards to be specified in national law in accordance with the Charter of Fundamental Rights of the European

([22]) 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).

([23]) Regulation (EU) 2021/1149 of the European Parliament and of the Council of 7 July 2021 establishing the Internal Security Fund (OJ L 251, 15.7.2021, p. 94).

([24]) Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013 (OJ L 170, 12.5.2021, p. 1).

Union. When assessing the compliance of a critical entity with its obligations as laid down in this Directive, the competent authorities under this Directive should be able to request the competent authorities under Directive (EU) 2022/2555 to exercise their supervisory and enforcement powers in relation to an entity under that Directive that has been identified as a critical entity under this Directive. The competent authorities under this Directive and the competent authorities under Directive (EU) 2022/2555 should cooperate and exchange information for that purpose.

(41) In order to apply this Directive in an effective and consistent manner, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to supplement this Directive by drawing up a list of essential services. That list should be used by competent authorities for the purpose of conducting Member State risk assessments and identifying critical entities pursuant to this Directive. In light of the minimum harmonisation approach of this Directive, that list is non-exhaustive, and Member States could complement it with additional essential services at national level in order to take into account national specificities in the provision of essential services. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making ([25]). 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.

(42) 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 ([26]).

(43) Since the objectives of this Directive, namely to ensure that services essential for the maintenance of vital societal functions or economic activities are provided in an unobstructed manner in the internal market 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.

(44) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council ([27]) and delivered an opinion on 11 August 2021.

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

([25]) OJ L 123, 12.5.2016, p. 1.

([26]) 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).

([27]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. This Directive:

(a) lays down obligations on Member States to take specific measures aimed at ensuring that services which are essential for the maintenance of vital societal functions or economic activities within the scope of Article 114 TFEU are provided in an unobstructed manner in the internal market, in particular obligations to identify critical entities and to support critical entities in meeting the obligations imposed on them;

(b) lays down obligations for critical entities aimed at enhancing their resilience and ability to provide services as referred to in point (a) in the internal market;

(c) establishes rules:

(i) on the supervision of critical entities;

(ii) on enforcement;

(iii) for the identification of critical entities of particular European significance and on advisory missions to assess the measures that such entities have put in place to meet their obligations under Chapter III;

(d) establishes common procedures for cooperation and reporting on the application of this Directive;

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

2. This Directive shall not apply to matters covered by Directive (EU) 2022/2555, without prejudice to Article 8 of this Directive. In light of the relationship between the physical security and cybersecurity of critical entities, Member States shall ensure that this Directive and Directive (EU) 2022/2555 are implemented in a coordinated manner.

3. Where provisions of sector-specific Union legal acts require critical entities to take measures to enhance their resilience and where those requirements are recognised by Member States as at least equivalent to the corresponding obligations laid down in this Directive, the relevant provisions of this Directive, including the provisions on supervision and enforcement laid down in Chapter VI, shall not apply.

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

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

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

7. Member States may decide that Article 11 and Chapters III, IV and VI, in whole or in part, do not apply to specific critical entities which carry out activities in the areas of national security, public security, defence or law enforcement, including the investigation, detection and prosecution of criminal offences, or which provide services exclusively to the public administration entities referred to in paragraph 6 of this Article.

8. The obligations laid down in this Directive shall not entail the supply of information the disclosure of which would be contrary to the essential interests of Member States' national security, public security or defence.

9. This Directive is without prejudice to Union law on the protection of personal data, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council ([28]) and Directive 2002/58/EC of the European Parliament and of the Council ([29]).

Article 2

Definitions

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

(1) 'critical entity' means a public or private entity which has been identified by a Member State in accordance with Article 6 as belonging to one of the categories set out in the third column of the table in the Annex;

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

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

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

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

(6) 'risk' means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident;

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

(8) 'standard' means a standard as defined in Article 2, point (1), of Regulation (EU) No 1025/2012 of the European Parliament and of the Council ([30]);

([28]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

([29]) 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 (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

([30]) Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).

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

(10) 'public administration entity' means an entity recognised as such in a Member State in accordance with national law, not including the judiciary, parliaments or central banks, which complies with the following criteria:

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

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

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

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

Article 3

Minimum harmonisation

This Directive shall not preclude Member States from adopting or maintaining provisions of national law with a view to achieving a higher level of resilience of critical entities, provided that such provisions are consistent with Member States' obligations laid down in Union law.

CHAPTER II

NATIONAL FRAMEWORKS ON THE RESILIENCE OF CRITICAL ENTITIES

Article 4

Strategy on the resilience of critical entities

1. Following a consultation that is, to the extent practically possible, open to relevant stakeholders, each Member State shall adopt by 17 January 2026 a strategy for enhancing the resilience of critical entities (the 'strategy'). The strategy shall set out strategic objectives and policy measures, building upon relevant existing national and sectoral strategies, plans or similar documents, with a view to achieving and maintaining a high level of resilience on the part of critical entities and covering at least the sectors set out in the Annex.

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

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

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

(c) a description of measures necessary to enhance the overall resilience of critical entities, including a description of the risk assessment referred to in Article 5;

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

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

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

(g) a policy framework for coordination between the competent authorities under this Directive ('competent authorities') and the competent authorities under Directive (EU) 2022/2555 for the purposes of information sharing on cybersecurity risks, cyber threats and cyber incidents and non-cyber risks, threats and incidents and the exercise of supervisory tasks;

(h) a description of measures already in place which aim to facilitate the implementation of obligations under Chapter III of this Directive by small and medium-sized enterprises within the meaning of the Annex to Commission Recommendation 2003/361/EC ([31]) that the Member State in question has identified as critical entities.

Following a consultation that is, to the extent practically possible, open to relevant stakeholders, Member States shall update their strategies at least every four years.

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

Article 5

Risk assessment by Member States

1. The Commission is empowered to adopt a delegated act, in accordance with Article 23, by 17 November 2023 to supplement this Directive by establishing a non-exhaustive list of essential services in the sectors and subsectors set out in the Annex. The competent authorities shall use that list of essential services for the purpose of carrying out a risk assessment ('Member State risk assessment') by 17 January 2026, whenever necessary subsequently, and at least every four years. The competent authorities shall use Member State risk assessments for the purpose of identifying critical entities in accordance with Article 6 and assisting those critical entities to take measures pursuant to Article 13.

Member State risk assessments shall account for the relevant natural and man-made risks, including those of a cross-sectoral or cross-border nature, accidents, natural disasters, public health emergencies and hybrid threats or other antagonistic threats, including terrorist offences as provided for in Directive (EU) 2017/541 of the European Parliament and of the Council ([32]).

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

(a) the general risk assessment carried out pursuant to Article 6(1) of Decision No 1313/2013/EU;

(b) other relevant risk assessments, carried out in accordance with the requirements of the relevant sector-specific Union legal acts, including Regulations (EU) 2017/1938 ([33]) and (EU) 2019/941 ([34]) of the European Parliament and of the Council and Directives 2007/60/EC ([35]) and 2012/18/EU ([36]) of the European Parliament and of the Council;

([31]) Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).
([32]) 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).
([33]) 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).
([34]) 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).
([35]) 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).
([36]) 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).

(c) the relevant risks arising from the extent to which the sectors set out in the Annex depend on one another, including from the extent to which they depend on entities located within other Member States and third countries, and the impact that a significant disruption in one sector may have on other sectors, including any significant risks to citizens and the internal market;

(d) any information on incidents notified in accordance with Article 15.

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

3. Member States shall make the relevant elements of Member State risk assessments available, where relevant through their single points of contact, to the critical entities that they have identified in accordance with Article 6. Member States shall ensure that the information provided to critical entities assists them in carrying out their risk assessments pursuant to Article 12 and in taking measures to ensure their resilience pursuant to Article 13.

4. Within three months of carrying out a Member State risk assessment, a Member State shall provide the Commission with relevant information on the types of risks identified following, and the outcomes of, that Member State risk assessment, per sector and subsector set out in the Annex.

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

Article 6

Identification of critical entities

1. By 17 July 2026, each Member State shall identify the critical entities for the sectors and subsectors set out in the Annex.

2. When a Member State identifies critical entities pursuant to paragraph 1, it shall take into account the outcomes of its Member State risk assessment and its strategy and shall apply all of the following criteria:

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

(b) the entity operates, and its critical infrastructure is located, on the territory of that Member State; and

(c) an incident would have significant disruptive effects, as determined in accordance with Article 7(1), on the provision by the entity of one or more essential services or on the provision of other essential services in the sectors set out in the Annex that depend on that or those essential services.

3. Each Member State shall establish a list of the critical entities identified pursuant to paragraph 2 and ensure that those critical entities are notified that they have been identified as critical entities within one month of that identification. Member States shall inform those critical entities of their obligations under Chapters III and IV and the date from which those obligations apply to them, without prejudice to Article 8. Member States shall inform critical entities in the sectors set out in points 3, 4 and 8 of the table in the Annex that they have no obligations under Chapters III and IV, unless national measures provide otherwise.

For the critical entities concerned, Chapter III shall apply from 10 months after the date of the notification referred to in the first subparagraph of this paragraph.

4. Member States shall ensure that their competent authorities under this Directive notify the competent authorities under Directive (EU) 2022/2555 of the identity of the critical entities that they have identified under this Article within one month of that identification. That notification shall specify, where applicable, that the critical entities concerned are entities in the sectors set out in points 3, 4 and 8 of the table in the Annex to this Directive and have no obligations under Chapters III and IV thereof.

5. 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 referred to in paragraph 3. Where those updates lead to the identification of additional critical entities, paragraphs 3 and 4 shall apply to those additional critical entities. In addition, Member States shall ensure that entities that are no longer identified as critical entities following any such update are notified in due time of that fact and the fact that they are no longer subject to the obligations under Chapter III from the date of receipt of that notification.

6. The Commission shall, in cooperation with the Member States, develop recommendations and non-binding guidelines to support Member States in identifying critical entities.

Article 7

Significant disruptive effect

1. When determining the significance of a disruptive effect as referred to in Article 6(2), point (c), Member States shall take into account the following criteria:

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

(b) the extent to which other sectors and subsectors as set out in the Annex depend on the essential service in question;

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

(d) the entity's market share in the market for the essential service or essential services concerned;

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

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

2. After the identification of the critical entities under Article 6(1), each Member State shall submit the following information to the Commission without undue delay:

(a) a list of essential services in that Member State where there are any additional essential services as compared to the list of essential services referred to in Article 5(1);

(b) the number of critical entities identified for each sector and subsector set out in the Annex and for each essential service;

(c) any thresholds applied to specify one or more of the criteria in paragraph 1.

Thresholds as referred to in the first subparagraph, point (c), may be presented as such or in aggregated form.

Member States shall subsequently submit information referred to in the first subparagraph whenever necessary and at least every four years.

3. The Commission shall, after consulting the Critical Entities Resilience Group referred to in Article 19, adopt non-binding guidelines to facilitate the application of the criteria referred to in paragraph 1 of this Article, taking into account the information referred to in paragraph 2 of this Article.

Article 8

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

Member States shall ensure that Article 11 and Chapters III, IV and VI do not apply to critical entities that they have identified in the sectors set out in points 3, 4 and 8 of the table in the Annex. Member States may adopt or maintain provisions of national law to achieve a higher level of resilience for those critical entities, provided that those provisions are consistent with applicable Union law.

Article 9

Competent authorities and single point of contact

1. Each Member State shall designate or establish one or more competent authorities responsible for the correct application and, where necessary, enforcement of the rules set out in this Directive at national level.

As regards the critical entities in the sectors set out in points 3 and 4 of the table in the Annex to this Directive, the competent authorities shall, in principle, be the competent authorities referred to in Article 46 of Regulation (EU) 2022/2554. As regards the critical entities in the sector set out in point 8 of the table in the Annex to this Directive, the competent authorities shall, in principle, be the competent authorities under Directive (EU) 2022/2555. Member States may designate a different competent authority for the sectors set out in points 3, 4 and 8 of the table in the Annex to this Directive in accordance with existing national frameworks.

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

2. Each Member State shall designate or establish one single point of contact to exercise a liaison function for the purpose of ensuring cross-border cooperation with the single points of contact of other Member States and the Critical Entities Resilience Group referred to in Article 19 ('single point of contact'). Where relevant, a Member State shall designate its single point of contact within a competent authority. Where relevant, a Member State may provide that its single point of contact also exercise a liaison function with the Commission and ensure cooperation with third countries.

3. By 17 July 2028, and every two years thereafter, the single points of contact shall submit a summary report to the Commission and to the Critical Entities Resilience Group referred to in Article 19 on the notifications they have received, including the number of notifications, the nature of notified incidents and the actions taken in accordance with Article 15(3).

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

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

5. Each Member State shall ensure that its competent authority, whenever appropriate, and in accordance with Union and national law, consults and cooperates with other relevant national authorities, including those in charge of civil protection, law enforcement and the protection of personal data, and with critical entities and relevant interested parties.

6. Each Member State shall ensure that its competent authority under this Directive cooperates and exchanges information with competent authorities under Directive (EU) 2022/2555 on cybersecurity risks, cyber threats and cyber incidents and non-cyber risks, threats and incidents affecting critical entities, including with regard to relevant measures its competent authority and competent authorities under Directive (EU) 2022/2555 have taken.

7. Within three months of the designation or establishment of the competent authority and the single point of contact, each Member State shall notify the Commission of their identity and their tasks and responsibilities under this Directive, their contact details and any subsequent change thereto. Member States shall inform the Commission where they decide to designate an authority other than the competent authorities referred to in paragraph 1, second subparagraph, as the competent authorities in respect of the critical entities in the sectors set out in points 3, 4 and 8 of the table in the Annex. Each Member State shall make public the identity of its competent authority and single point of contact.

8. The Commission shall make a list of the single points of contact publicly available.

Article 10

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 the personnel of critical entities. Without prejudice to applicable rules on State aid, Member States may provide financial resources to critical entities, where necessary and justified by public interest objectives.

2. Each Member State shall ensure that its competent authority cooperates and exchanges information and good practices with critical entities of the sectors set out in the Annex.

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

Article 11

Cooperation between Member States

1. Whenever appropriate, Member States shall consult one another regarding critical entities for the purpose of ensuring that this Directive is applied in a consistent manner. Such consultations shall take place, in particular, regarding critical entities that:

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

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

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

2. The consultations referred to in paragraph 1 shall aim at enhancing the resilience of critical entities and, where possible, reducing the administrative burden on them.

CHAPTER III

RESILIENCE OF CRITICAL ENTITIES

Article 12

Risk assessment by critical entities

1. Notwithstanding the deadline set out in Article 6(3), second subparagraph, Member States shall ensure that critical entities carry out a risk assessment within nine months of receiving the notification referred to in Article 6(3), whenever necessary subsequently, and at least every four years, on the basis of Member State risk assessments and other relevant sources of information, in order to assess all relevant risks that could disrupt the provision of their essential services ('critical entity risk assessment').

2. Critical entity risk assessments shall account for all the relevant natural and man-made risks which could lead to an incident, including those of a cross-sectoral or cross-border nature, accidents, natural disasters, public health emergencies and hybrid threats and other antagonistic threats, including terrorist offences as provided for in Directive (EU) 2017/541. A critical entity risk assessment shall take into account the extent to which other sectors as set out in the Annex depend on the essential service provided by the critical entity and the extent to which that critical entity depends on essential services provided by other entities in such other sectors, including, where relevant, in neighbouring Member States and third countries.

Where a critical entity has carried out other risk assessments or drawn up documents pursuant to obligations laid down in other legal acts that are relevant for its critical entity risk assessment, it may use those assessments and documents to meet the requirements set out in this Article. When exercising its supervisory functions, the competent authority may declare an existing risk assessment carried out by a critical entity that addresses the risks and extent of dependence referred to in the first subparagraph of this paragraph as compliant, in whole or in part, with the obligations under this Article.

Article 13

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, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:

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

(b) ensure adequate physical protection of their premises and critical infrastructure, duly considering, for example, fencing, barriers, perimeter monitoring tools and routines, detection equipment and access controls;

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

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

(e) ensure adequate employee security management, duly considering measures such as setting out categories of personnel who exercise critical functions, establishing access rights to premises, critical infrastructure and sensitive information, setting up procedures for background checks in accordance with Article 14 and designating the categories of persons who are required to undergo such background checks, and laying down appropriate training requirements and qualifications;

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

For the purposes of the first subparagraph, point (e), Member States shall ensure that critical entities take into account the personnel of external service providers when setting out categories of personnel who exercise critical functions.

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

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

4. At the request of the Member State that has 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 18(6), (8) and (9), to provide advice to the critical entity concerned in meeting its obligations under Chapter III. The advisory mission shall report its findings to the Commission, that Member State and the critical entity concerned.

5. The Commission shall, after consulting the Critical Entities Resilience Group referred to in Article 19, adopt non-binding guidelines to further specify the technical, security and organisational measures that may be taken pursuant to paragraph 1 of this Article.

6. 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 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 24(2).

Article 14

Background checks

1. Member States shall specify the conditions under which a critical entity is permitted, in duly reasoned cases and taking into account the Member State risk assessment, to submit requests for background checks on persons who:

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

(b) are authorised to directly or remotely access its premises, information or control systems, including in connection with the security of the critical entity;

(c) are under consideration for recruitment to positions that fall under the criteria set out in point (a) or (b).

2. Requests as referred to in paragraph 1 of this Article shall be assessed within a reasonable timeframe and processed in accordance with national law and procedures and relevant and applicable Union law, including Regulation (EU) 2016/679 and Directive (EU) 2016/680 of the European Parliament and of the Council ([37]). Background checks shall be proportionate and strictly limited to what is necessary. They shall be carried out for the sole purpose of evaluating a potential security risk to the critical entity concerned.

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

(a) corroborate the identity of the person who is the subject of the background check;

(b) check the criminal records of that person with regards to offences which would be relevant for a specific position.

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

([37]) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

Article 15

Incident notification

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

(a) the number and proportion of users affected by the disruption;

(b) the duration of the disruption;

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

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

2. Notifications as referred to in paragraph 1, first subparagraph, shall include any available information necessary to enable the competent authority to understand the nature, cause and possible consequences of the incident, including any available information necessary to determine any cross-border impact of the incident. Such notifications shall not subject critical entities to increased liability.

3. On the basis of the information provided by a critical entity in a notification as referred to in paragraph 1, the relevant competent authority, via the single point of contact, shall inform the single point of contact of other affected Member States where the incident has or might have a significant impact on critical entities and the continuity of the provision of essential services to or in one or more other Member States.

Single points of contact sending and receiving information pursuant to the first subparagraph shall, in accordance with Union or national law, treat that 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 following a notification as referred to in paragraph 1, the competent authority concerned shall provide the critical entity concerned with relevant follow-up information, including information that could support that critical entity's effective response to the incident in question. Member States shall inform the public where they determine that it would be in the public interest to do so.

Article 16

Standards

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

CHAPTER IV

CRITICAL ENTITIES OF PARTICULAR EUROPEAN SIGNIFICANCE

Article 17

Identification of critical entities of particular European significance

1. An entity shall be considered a critical entity of particular European significance where it:

(a) has been identified as a critical entity pursuant to Article 6(1);

(b) provides the same or similar essential services to or in six or more Member States; and

(c) has been notified pursuant to paragraph 3 of this Article.

2. Member States shall ensure that a critical entity, following the notification referred to in Article 6(3), informs its competent authority where it provides essential services to or in six or more Member States. In such a case, Member States shall ensure that the critical entity informs its competent authority of the essential services it provides to or in those Member States and of the Member States to which or in which it provides such essential services. Member States shall notify the Commission, without undue delay, of the identity of such critical entities and of the information they provide under this paragraph.

The Commission shall consult the competent authority of the Member State which identified a critical entity as referred to in the first subparagraph, the competent authority of other Member States concerned and the critical entity in question. During those consultations, each Member State shall inform the Commission where it deems that the services provided to that Member State by the critical entity are essential services.

3. Where the Commission establishes, on the basis of the consultations referred to in paragraph 2 of this Article, that the critical entity concerned provides essential services to or in six or more Member States, the Commission shall notify that critical entity, through its competent authority, that it is considered a critical entity of particular European significance and inform that critical entity of its obligations under this Chapter and the date from which those obligations apply to it. Once the Commission informs the competent authority of its decision to consider a critical entity as a critical entity of particular European significance, the competent authority shall forward that notification to that critical entity without undue delay.

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

Article 18

Advisory missions

1. At the request of the Member State that has identified a critical entity of particular European significance as a critical entity pursuant to Article 6(1), the Commission shall organise an advisory mission to assess the measures that that critical entity has put in place to meet its obligations under Chapter III.

2. On its own initiative or at the request of one or more Member States to or in which the essential service is provided, and provided that the Member State that has identified a critical entity of particular European significance as a critical entity pursuant to Article 6(1) so agrees, the Commission shall organise an advisory mission as referred to in paragraph 1 of this Article.

3. On a reasoned request from the Commission or from one or more Member States to or in which the essential service is provided, the Member State that has identified a critical entity of particular European significance as a critical entity pursuant to Article 6(1) shall provide the following to the Commission:

(a) the relevant parts of the critical entity risk assessment;

(b) a list of relevant measures taken in accordance with Article 13;

(c) supervisory or enforcement actions, including assessments of compliance or orders issued, that its competent authority has undertaken pursuant to Articles 21 and 22 in respect of that critical entity.

4. The advisory mission shall report its findings to the Commission, to the Member State that has identified a critical entity of particular European significance as a critical entity pursuant to Article 6(1), to the Member States to or in which the essential service is provided and to the critical entity concerned within three months of the conclusion of the advisory mission.

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

The Commission shall, based on the advice referred to in the second subparagraph of this paragraph, communicate its opinion to the Member State that has identified a critical entity of particular European significance as a critical entity pursuant to Article 6(1), to the Member States to or in which the essential service is provided and to that critical entity as to whether that critical entity complies with its obligations under Chapter III and, where appropriate, as to the measures which could be taken to improve the resilience of that critical entity.

The Member State that has identified a critical entity of particular European significance as a critical entity pursuant to Article 6(1) shall ensure that its competent authority and the critical entity concerned take into account the opinion referred to in the third subparagraph of this paragraph and provide information to the Commission and the Member States to or in which the essential service is provided on the measures it has taken pursuant to that opinion.

5. Each advisory mission shall consist of experts from the Member State in which the critical entity of particular European significance is located, experts from the Member States to or in which the essential service is provided, and Commission representatives. Those Member States may propose candidates to be part of an advisory mission. The Commission shall, following a consultation with the Member State that has identified a critical entity of particular European significance as a critical entity pursuant to Article 6(1), select and appoint the members of each advisory mission in accordance with their professional capacity and ensuring, where possible, a geographically balanced representation from all those Member States. Whenever necessary, members of the advisory mission shall have valid and appropriate security clearance. The Commission shall bear the costs related to participation in advisory missions.

The Commission shall organise the programme of each advisory mission, in consultation with the members of the advisory mission in question and in agreement with the Member State that has identified a critical entity of particular European significance as a critical entity pursuant to Article 6(1).

6. The Commission shall adopt an implementing act laying down rules on the procedural arrangements for requests to organise advisory missions, for handling such requests, for the conduct and reports of advisory missions and for handling the communication of the Commission's opinion referred to in paragraph 4, third subparagraph, of this Article and of the measures taken, duly taking into account the confidentiality and commercial sensitivity of the information concerned. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 24(2).

7. Member States shall ensure that critical entities of particular European significance provide advisory missions with access to information, systems and facilities relating to the provision of their essential services necessary for carrying out the advisory mission concerned.

8. Advisory missions shall be carried out in compliance with the applicable national law of the Member State in which they take place, with respect for that Member State's responsibility for national security and the protection of its security interests.

9. When organising advisory missions, the Commission shall take into account the reports of any inspections carried out by the Commission under Regulations (EC) No 725/2004 and (EC) No 300/2008 and the reports of any monitoring carried out by the Commission under Directive 2005/65/EC in respect of the critical entity concerned.

10. The Commission shall inform the Critical Entities Resilience Group referred to in Article 19 whenever an advisory mission is organised. The Member State in which the advisory mission took place and the Commission shall also inform the Critical Entities Resilience Group of the main findings of the advisory mission and the lessons learned with a view to promoting mutual learning.

CHAPTER V

COOPERATION AND REPORTING

Article 19

Critical Entities Resilience Group

1. A Critical Entities Resilience Group is hereby established. The Critical Entities Resilience Group shall support the Commission and facilitate cooperation among Member States and the exchange of information on issues relating to this Directive.

2. The Critical Entities Resilience Group shall be composed of representatives of the Member States and the Commission who hold security clearance, where appropriate. Where relevant for the performance of its tasks, the Critical Entities Resilience Group may invite relevant stakeholders to participate in its work. Where requested by the European Parliament, the Commission may invite experts from the European Parliament to attend meetings of the Critical Entities Resilience Group.

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

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

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

(b) analysing the strategies in order to identify best practices in respect of the strategies;

(c) facilitating the exchange of best practices with regard to the identification of critical entities by the Member States pursuant to Article 6(1), including in relation to cross-border and cross-sectoral dependencies and regarding risks and incidents;

(d) where appropriate, contributing on issues relating to this Directive to documents concerning resilience at Union level;

(e) contributing to the preparation of the guidelines referred to in Article 7(3) and Article 13(5) and, upon request, any delegated or implementing acts adopted pursuant to this Directive;

(f) analysing the summary reports referred to in Article 9(3) with a view to promoting the sharing of best practices on the action taken in accordance with Article 15(3);

(g) exchanging best practices related to the notification of incidents referred to in Article 15;

(h) discussing the summary reports of advisory missions and the lessons learned in accordance with Article 18(10);

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

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

4. By 17 January 2025 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. That work programme shall be consistent with the requirements and objectives of this Directive.

5. The Critical Entities Resilience Group shall meet on a regular basis and in any event at least once a year with the Cooperation Group established under Directive (EU) 2022/2555 to promote and facilitate cooperation and the exchange of information.

6. The Commission may adopt implementing acts laying down procedural arrangements necessary for the functioning of the Critical Entities Resilience Group, respecting Article 1(4). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 24(2).

7. The Commission shall provide the Critical Entities Resilience Group with a summary report of the information provided by the Member States pursuant to Article 4(3) and Article 5(4) by 17 January 2027, whenever necessary subsequently, and at least every four years.

Article 20

Commission support to competent authorities and critical entities

1. The Commission shall, where appropriate, support Member States and critical entities in complying with their obligations under this Directive. The Commission shall prepare a Union-level overview of cross-border and cross-sectoral risks to the provision of essential services, organise advisory missions as referred to in Article 13(4) and Article 18 and facilitate information exchange among Member States and experts across the Union.

2. The Commission shall complement Member States' activities as referred to in Article 10 by developing best practices, guidance materials and methodologies, and cross-border training activities and exercises to test the resilience of critical entities.

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

CHAPTER VI

SUPERVISION AND ENFORCEMENT

Article 21

Supervision and enforcement

1. In order to assess the compliance of the entities identified by Member States as critical entities pursuant to Article 6(1) with the obligations laid down in this Directive, Member States shall ensure that the competent authorities 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 measures taken by critical entities in accordance with Article 13;

(b) conduct or order audits in respect of critical 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 under Directive (EU) 2022/2555 that Member States have identified as critical entities under this Directive provide, within a reasonable time limit set by those authorities:

(a) the information necessary to assess whether the measures taken by those entities to ensure their resilience meet the requirements set out in Article 13;

(b) evidence of the effective implementation of those measures, including the results of an audit conducted by an independent and qualified 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 22, the competent authorities may, following the supervisory actions referred to in paragraph 1 of this Article or the assessment of the information referred to in paragraph 2 of this Article, order the critical entities concerned to take the necessary and proportionate measures to remedy any identified infringement of this Directive, within a reasonable time limit set by those authorities, and to provide those authorities with 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 of the critical entities affected, such as the protection of trade and business secrets, are duly safeguarded, including the right to be heard, the right of defence and the right to an effective remedy before an independent court.

5. Member States shall ensure that, where a competent authority under this Directive assesses the compliance of a critical entity pursuant to this Article, that competent authority informs the competent authorities of the Member States concerned under Directive (EU) 2022/2555. For that purpose, Member States shall ensure that competent authorities under this Directive can request the competent authorities under Directive (EU) 2022/2555 to exercise their supervisory and enforcement powers in relation to an entity under that Directive that has been identified as a critical entity under this Directive. For that purpose, Member States shall ensure that competent authorities under this Directive cooperate and exchange information with the competent authorities under Directive (EU) 2022/2555.

Article 22

Penalties

Member States shall lay down the rules on penalties applicable to infringements of the national measures 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, by 17 October 2024, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.

CHAPTER VII

DELEGATED AND IMPLEMENTING ACTS

Article 23

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 5(1) shall be conferred on the Commission for a period of five years from 16 January 2023.

3. The delegation of power referred to in Article 5(1) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

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

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

6. A delegated act adopted pursuant to Article 5(1) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 24

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.

CHAPTER VIII

FINAL PROVISIONS

Article 25

Reporting and review

By 17 July 2027, the Commission shall submit to the European Parliament and to the Council a report assessing the extent to which each Member State has taken the necessary measures to comply with this Directive.

The Commission shall periodically review the functioning of this Directive and report to the European Parliament and to the Council. That report shall, in particular, assess the added value of this Directive, its impact on ensuring the resilience of critical entities and whether the Annex to this Directive should be modified. The Commission shall submit the first such report by 17 June 2029. For the purpose of reporting under this Article, the Commission shall take into account relevant documents of the Critical Entities Resilience Group.

Article 26

Transposition

1. By 17 October 2024, Member States shall adopt and publish the measures necessary to comply with this Directive. They shall immediately inform the Commission thereof.

They shall apply those measures from 18 October 2024.

2. When Member States adopt the measures referred to in paragraph 1, they shall contain a reference to this Directive or be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

Article 27

Repeal of Directive 2008/114/EC

Directive 2008/114/EC is repealed with effect from 18 October 2024.

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

Article 28

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 29

Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 14 December 2022.

For the European Parliament	*For the Council*
The President	*The President*
R. METSOLA	M. BEK

ANNEX

SECTORS, SUBSECTORS AND CATEGORIES OF ENTITIES

Sectors	Subsectors	Categories of entities
1. Energy	(a) Electricity	— Electricity undertakings as defined in Article 2, point (57), of Directive (EU) 2019/944 of the European Parliament and of the Council ([1]), which carry out the function of 'supply' as defined in Article 2, point (12), of that Directive
		— Distribution system operators as defined in Article 2, point (29), of Directive (EU) 2019/944
		— Transmission system operators as defined in Article 2, point (35), of Directive (EU) 2019/944
		— Producers as defined in Article 2, point (38), of Directive (EU) 2019/944
		— Nominated electricity market operators as defined in Article 2, point (8), of Regulation (EU) 2019/943 of the European Parliament and of the Council ([2])
		— Market participants as defined in Article 2, point (25), of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services as defined in Article 2, points (18), (20) and (59), of Directive (EU) 2019/944
	(b) District heating and cooling	— Operators of district heating or district cooling as defined in Article 2, point (19), of Directive (EU) 2018/2001 of the European Parliament and of the Council ([3])
	(c) Oil	— Operators of oil transmission pipelines
		— Operators of oil production, refining and treatment facilities, storage and transmission
		— Central stockholding entities as defined in Article 2, point (f), of Council Directive 2009/119/EC ([4])

Sectors	Subsectors	Categories of entities
	(d) Gas	— Supply undertakings as defined in Article 2, point (8), of Directive 2009/73/EC of the European Parliament and of the Council ([5])
		— Distribution system operators as defined in Article 2, point (6), of Directive 2009/73/EC
		— Transmission system operators as defined in Article 2, point (4), of Directive 2009/73/EC
		— Storage system operators as defined in Article 2, point (10), of Directive 2009/73/EC
		— LNG system operators as defined in Article 2, point (12), of Directive 2009/73/EC
		— Natural gas undertakings as defined in Article 2, point (1), of Directive 2009/73/EC
		— Operators of natural gas refining and treatment facilities
	(e) Hydrogen	— Operators of hydrogen production, storage and transmission
2. Transport	(a) Air	— Air carriers as defined in Article 3, point (4), of Regulation (EC) No 300/2008 used for commercial purposes
		— Airport managing bodies as defined in Article 2, point (2), of Directive 2009/12/EC of the European Parliament and of the Council ([6]), airports as defined in Article 2, point (1), of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council ([7]), and entities operating ancillary installations contained within airports
		— Traffic management control operators providing air traffic control (ATC) services as defined in Article 2, point (1), of Regulation (EC) No 549/2004 of the European Parliament and of the Council ([8])

Sectors	Subsectors	Categories of entities
	(b) Rail	— Infrastructure managers as defined in Article 3, point (2), of Directive 2012/34/EU of the European Parliament and of the Council ([9])
		— Railway undertakings as defined in Article 3, point (1), of Directive 2012/34/EU and operators of service facilities as defined in Article 3, point (12), of that Directive
	(c) Water	— Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to Regulation (EC) No 725/2004, not including the individual vessels operated by those companies
		— Managing bodies of ports as defined in Article 3, point (1), of Directive 2005/65/EC, including their port facilities as defined in Article 2, point (11), of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports
		— Operators of vessel traffic services (VTS) as defined in Article 3, point (o), of Directive 2002/59/EC of the European Parliament and of the Council ([10])
	(d) Road	— Road authorities as defined in Article 2, point (12), of Commission Delegated Regulation (EU) 2015/962 ([11]) responsible for traffic management control, excluding public entities for whom traffic-management or the operation of intelligent transport systems is a non-essential part of their general activity
		— Operators of Intelligent Transport Systems as defined in Article 4, point (1), of Directive 2010/40/EU of the European Parliament and of the Council ([12])
	(e) public transport	— Public service operators as defined in Article 2, point (d), of Regulation (EC) No 1370/2007 of the European Parliament and of the Council ([13])
3. Banking		— Credit institutions as defined in Article 4, point (1), of Regulation (EU) No 575/2013
4. Financial market infrastructure		— Operators of trading venues as defined in Article 4, point (24), of Directive 2014/65/EU
		— Central counterparties (CCPs) as defined in Article 2, point (1), of Regulation (EU) No 648/2012

Sectors	Subsectors	Categories of entities
5. Health		— Healthcare providers as defined in Article 3, point (g), of Directive 2011/24/EU of the European Parliament and of the Council ([14])
		— EU reference laboratories as referred to in Article 15 of Regulation (EU) 2022/2371 of the European Parliament and of the Council ([15])
		— Entities carrying out research and development activities of medicinal products as defined in Article 1, point (2), of Directive 2001/83/EC of the European Parliament and of the Council ([16])
		— Entities manufacturing basic pharmaceutical products and pharmaceutical preparations as referred to in Section C division 21 of NACE Rev. 2
		— Entities manufacturing medical devices considered as critical during a public health emergency ('public health emergency critical devices list') within the meaning of Article 22 of Regulation (EU) 2022/123 of the European Parliament and of the Council ([17])
		— Entities holding a distribution authorisation as referred to in Article 79 of Directive 2001/83/EC
6. Drinking water		— Suppliers and distributors of water intended for human consumption as defined in Article 2, point (1)(a), of Directive (EU) 2020/2184 of the European Parliament and of the Council ([18]), excluding distributors for which distribution of water for human consumption is a non-essential part of their general activity of distributing other commodities and goods
7. Waste water		— Undertakings collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water as defined in Article 2, points (1), (2) and (3), of Council Directive 91/271/EEC ([19]), excluding undertakings for which collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water is a non-essential part of their general activity

Sectors	Subsectors	Categories of entities
8. Digital infrastructure		— Providers of internet exchange points as defined in Article 6, point (18), of Directive (EU) 2022/2555
		— DNS service providers as defined in Article 6, point (20), of Directive (EU) 2022/2555, excluding operators of root name servers
		— top-level-domain name registries as defined in Article 6, point (21), of Directive (EU) 2022/2555
		— Providers of cloud computing services as defined in Article 6, point (30), of Directive (EU) 2022/2555
		— Providers of data centre services as defined in Article 6, point (31), of Directive (EU) 2022/2555
		— Providers of content delivery networks as defined in Article 6, point (32), of Directive (EU) 2022/2555
		— Trust service providers as defined in Article 3, point (19), of Regulation (EU) No 910/2014 of the European Parliament and of the Council ([20])
		— Providers of public electronic communications networks as defined in Article 2, point (8), of Directive (EU) 2018/1972 of the European Parliament and of the Council ([21])
		— Providers of electronic communications services as defined in Article 2, point (4), of Directive (EU) 2018/1972 insofar as their services are publicly available
9. Public administration		— Public administration entities of central governments as defined by Member States in accordance with national law
10. Space		— Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks as defined in Article 2, point (8), of Directive (EU) 2018/1972

Sectors	Subsectors	Categories of entities
11. Production, processing and distribution of food		— Food businesses as defined in Article 3, point (2), of Regulation (EC) No 178/2002 of the European Parliament and of the Council ([22]) which are engaged exclusively in logistics and wholesale distribution and large scale industrial production and processing

([1]) Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019, p. 125).
([2]) Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (OJ L 158, 14.6.2019, p. 54).
([3]) Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (OJ L 328, 21.12.2018, p. 82).
([4]) Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products (OJ L 265, 9.10.2009, p. 9).
([5]) Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (OJ L 211, 14.8.2009, p. 94).
([6]) 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).
([7]) Regulation (EU) 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).
([8]) 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).
([9]) 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).
([10]) 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).
([11]) 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).
([12]) 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).
([13]) Regulation (EC) No 1370/2007 of the European Parliament and of the Council of 23 October 2007 on public passenger transport services by rail and by road and repealing Council Regulations (EEC) Nos 1191/69 and 1107/70 (OJ L 315, 3.12.2007, p. 1).
([14]) 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).
([15]) Regulation (EU) 2022/2371 of the European Parliament and of the Council of 23 November 2022 on serious cross-border threats to health and repealing Decision No 1082/2013/EU (OJ L 314, 6.12.2022, p. 26).
([16]) 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).
([17]) Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022 on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices (OJ L 20, 31.1.2022, p. 1).
([18]) Directive (EU) 2020/2184 of the European Parliament and of the Council of 16 December 2020 on the quality of water intended for human consumption (OJ L 435, 23.12.2020, p. 1).
([19]) Council Directive 91/271/EEC of 21 May 1991 concerning urban waste water treatment (OJ L 135, 30.5.1991, p. 40).
([20]) 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).
([21]) 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).
([22]) Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (OJ L 31, 1.2.2002, p. 1).