EUROPEAN
COMMISSION

Brussels, 16.12.2020
COM(2020) 829 final

2020/0365 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the resilience of critical entities

{SEC(2020) 433 final} - {SWD(2020) 358 final} - {SWD(2020) 359 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

To effectively protect Europeans, the European Union needs to continue to reduce vulnerabilities, including for the critical infrastructures that are essential for the functioning of our societies and economy. The livelihoods of European citizens and the good functioning of the internal market depend on different infrastructures for the reliable provision of services needed to maintain critical societal and economic activities. These services, vital under normal circumstances, are all the more important as Europe manages the effects of and looks towards recovering from the COVID-19 pandemic. It follows that entities providing essential services must be resilient, i.e. able to resist, absorb, accommodate to and recover from incidents that can lead to serious, potentially cross-sectoral and cross-border disruptions.

This proposal aims to enhance the provision in the internal market of services essential for the maintenance of vital societal functions or economic activities by increasing the resilience of critical entities providing such services. It reflects recent calls for action on the part of the Council[1] and the European Parliament,[2] both of which have encouraged the Commission to revise the current approach to better reflect the increased challenges to critical entities, and to ensure closer alignment with the Network and Information Systems (NIS) Directive[3]. This proposal is consistent and establishes close synergies with the proposed Directive on measures for a high common level of cybersecurity across the Union; ("NIS 2 Directive") which will replace the NIS Directive in order to address the increased interconnectedness between the physical and digital world through a legislative framework with robust resilience measures, both for cyber and physical aspects as set out in the Security Union Strategy[4].

Furthermore, the proposal reflects national approaches in an increasing number of Member States, which tend to emphasise cross-sectoral and cross-border interdependencies and are more and more informed by resilience thinking, in which protection is but one element alongside risk prevention and mitigation, business continuity and recovery. Given that critical infrastructures run the risk of also being potential terrorist targets, the measures aimed at ensuring the resilience of critical entities contained in this proposal contribute to the objectives of the recently adopted EU Agenda on Counter-Terrorism[5].

The European Union (EU) has long recognised the pan-European importance of critical infrastructures. For instance, the EU established the European Programme for Critical Infrastructure Protection (EPCIP) in 2006[6] and adopted the European Critical Infrastructure

---

1 Council Conclusions of 10 December 2019 on complementary efforts to enhance resilience and counter hybrid threats (14972/19).

2 Report on findings and recommendations of the European Parliament's Special Committee on Terrorism (2018/2044(INI)).

3 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.

4 COM(2020) 605.

5 COM(2020) 795.

6 Communication from the Commission on a European Programme for Critical Infrastructure Protection. COM (2006) 786.

(ECI) Directive in 2008.[7] The ECI Directive, which applies only to the energy and transport sectors, provides a procedure for identifying and designating ECIs, the disruption or destruction of which would have significant cross-border impacts in at least two Member States. It also sets out specific protection requirements on ECI operators and competent Member State authorities. To date, 94 ECIs have been designated, two-thirds of which are located in three Member States in Central and Eastern Europe. However, the scope of EU action on critical infrastructure resilience extends beyond these measures, and includes sectoral and cross-sectoral measures on *inter alia* climate proofing, civil protection, foreign direct investment and cybersecurity.[8] Meanwhile, Member States themselves have taken measures of their own in this area in ways that diverge from one another.

It is therefore apparent that the current framework on critical infrastructure protection is not sufficient to address the current challenges to critical infrastructures and the entities that operate them. Given the increasing interconnection among infrastructures, networks and operators delivering essential services across the internal market, it is necessary to fundamentally switch the current approach from protecting specific assets towards reinforcing the resilience of the critical entities that operate them.

The operational environment in which critical entities operate has changed significantly in recent years. Firstly, the risk landscape is more complex than in 2008, involving today natural hazards[9] (in many cases exacerbated by climate change), state-sponsored hybrid actions, terrorism, insider threats, pandemics, and accidents (such as industrial accidents). Secondly, operators are confronted with challenges in integrating new technologies such as 5G and unmanned vehicles into their operations, while at the same time addressing the vulnerabilities that such technologies could potentially create. Thirdly, these technologies and other trends make operators increasingly reliant on one another. The implications of this are clear – a disruption affecting the service provision by one operator in one sector has the potential to generate cascading effects on service provision in other sectors, and also potentially in other Member States or across the entire Union.

As evidenced by the 2019 evaluation of the ECI Directive[10], existing European and national measures face limitations in helping operators confront the operational challenges that they face today and the vulnerabilities that their interdependent nature entail.

There are several reasons for this, as set out in the impact assessment that supported the development of the proposal. Firstly, operators are not fully aware of or do not fully understand the implications of the dynamic risk landscape within which they operate. Secondly, resilience efforts diverge significantly between Member States and sectors. Thirdly, similar types of entities are recognised as being critical by some Member States but not by others, meaning that comparable entities receive varying degrees of official capacity-building support (in the form of, e.g. guidance, training and exercise organisation) depending on where they operate in the Union, and are subject to different requirements. The fact that the

---

7 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.

8 Communication from the Commission on an EU Strategy on adaptation to climate change. COM(2013) 216; Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism; Regulation 2019/452 establishing a framework for the screening of foreign direct investments into the Union; Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.

9 Overview of natural and man-made disaster risks the European Union may face. SWD(2020) 330.

10 SWD(2019) 308.

requirements and government support to operators varies from one Member State to another creates obstacles to operators when acting across borders, notably for those critical entities operating in Member States with more stringent frameworks. Given the increasingly interconnected nature of service provision and sectors in the Member States and across the EU, an insufficient level of resilience on the part of one operator poses a serious risk for entities elsewhere in the internal market.

Besides jeopardising the smooth functioning of the internal market, disruptions, especially those with cross-border and potentially pan-European implications, have possibly serious negative implications for citizens, business, governments and the environment. Indeed, at the individual level, disruptions may affect Europeans' ability to travel freely, work, and draw on essential public services like health care. In many cases, these and other core services that underpin daily life are provided by tightly interconnected networks of European businesses; a disruption to one business in one sector may have cascading effects across many other economic sectors. Finally, disruptions such as, for instance, large-scale power outages and serious transport accidents, may serve to erode security and public safety, prompting uncertainty and undermining confidence in critical entities, as well as in the authorities responsible for their oversight and for keeping the population safe and secure.

- **Consistency with existing provisions in the policy area**

This proposal reflects the priorities of the Commission's EU Security Union Strategy,[11] which calls for a revised approach to critical infrastructure resilience that better reflects the current and anticipated future risk landscape, the increasingly tight interdependencies between different sectors, and also the increasingly interdependent relationships between physical and digital infrastructures.

The proposed directive replaces the ECI Directive as well as accounts for and builds on other existing and envisaged instruments. The proposed directive constitutes a considerable change as compared to the ECI Directive, which applies only to the energy and transport sectors, focuses solely on protective measures, and provides a procedure for identifying and designating ECIs through cross-border dialogue. First of all, the proposed directive would have a much wider sectoral scope, covering ten sectors, namely energy, transport, banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure, public administration, and space. Secondly, the directive provides a procedure for Member States to identify critical entities using common criteria on the basis of a national risk assessment. Thirdly, the proposal sets out obligations on Member States and the critical entities that they identify, including ones with particular European significance, i.e. critical entities that provide essential services to or in more than one third of Member States that would be subject to specific oversight.

Where appropriate, the Commission would provide competent authorities and critical entities with support in complying with their obligations under the directive. In addition, the Critical Entities Resilience Group, which is a Commission expert group subject to the horizontal framework applicable to such groups, would provide advice to the Commission and promote strategic cooperation and the exchange of information. Finally, as the interdependencies do not stop at EU external borders, engagement with partner countries is also necessary. The proposed directive provides for a possibility of such cooperation, for instance in the area of risk assessments.

[11] Communication from the Commission on the EU Security Union Strategy. COM(2020) 605.

Consistency with other Union policies

The proposed directive has obvious links and is consistent with other sectoral and cross-sectoral EU initiatives on *inter alia* climate proofing, civil protection, foreign direct investment (FDI), cybersecurity and the financial services acquis. In particular, the proposal is closely aligned and establishes close synergies with the proposed NIS 2 Directive, which aims at enhancing all-hazards information and communication technology (ICT) resilience on the part of 'essential entities' and 'important entities' meeting specific thresholds in a large number of sectors. This proposal for a directive on the resilience of critical entities aims to ensure that competent authorities designated under this directive and those designated under the proposed NIS 2 Directive take complementary measures and exchange information as necessary regarding cyber and non-cyber resilience, and that particularly critical entities in the sectors considered to be 'essential' per the proposed NIS 2 Directive are also subject to more general resilience-enhancing obligations to address non-cyber risks. The physical security of network and information systems of entities in the digital infrastructure sector is addressed comprehensively in the proposed NIS 2 Directive as part of those entities' cybersecurity risk management and reporting obligations. In addition, the proposal builds on the existing financial services acquis, which establishes comprehensive requirements on financial entities to manage operational risks and ensure business continuity. Therefore, entities pertaining to the digital infrastructure, banking and financial infrastructure sectors should be treated as entities equivalent to critical entities pursuant to this Directive for the purposes of the obligations and activities of Member States while this Directive would not entail additional obligations on those entities.

The proposal also accounts for other sectoral and cross-sectoral initiatives on, e.g. civil protection, disaster risk reduction and climate change adaptation. Furthermore, the proposal recognises that in certain cases, existing EU legislation puts in place obligations on entities to address certain risk through protective measures. In such cases, e.g. on aviation or maritime security, the critical entities should describe those measures in their resilience plans. Furthermore, the proposed directive is without prejudice to the application of competition rules laid down in the Treaty on the Functioning of the European Union (TFEU).

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- **Legal basis**

Unlike Directive 2008/114/EC which was based on Article 308 of the Treaty esablishing the European Community (corresponding to the current Article 352 of the Treaty on the Functioning of the European Union, this proposal for a directive is based on Article 114 TFEU, which involves the approximation of laws for the improvement of the internal market. This is justified by the shift of the directive's aim, scope and content, increased interdependencies and the need to establish a more level playing field for critical entities. Instead of protecting a limited set of physical infrastructures the disruption or destruction of which would have significant cross-boder impacts, the aim is to enhance the resilience of entities in Member States which are critical for the provision of services which are essential for the maintenance of vital societal functions or economic activites in the internal market in a number of sectors underpinning the functioning of many other sectors of the economy of the Union. Because of the increased cross-border interdependencies between the services provided using critical infrastructures in those sectors, a disruption in one Member State may have implications in other Member States or the Union as a whole.

The current legal framework as established at Member State level regulating the services in question entails substantially diverging obligations, which are likely to increase. The diverging national rules to which critical entities are subject not only compromise the reliable provision of services across the internal market but also risk to negatively impact competition. This is principally due to the fact that similar types of entities providing similar types of services are considered as critical in some Member States but not in others. This means that entities that are, or that want to be, active in more than one Member State are subject to diverging obligations when acting across the internal market and that entities active in Member States with more stringent requirements may face obstacles compared to those in Member States with more lenient frameworks. These divergences are such that they have a direct negative effect on the functioning of the internal market.

- **Subsidiarity**

A common legislative framework at European level in this area is justified given the interdependent, cross-border nature of relationships between critical infrastructure operations and their outputs, i.e. essential services. Indeed, an operator situated in one Member State may provide services in several other Member States or across the entire EU through tightly intertwined networks. It follows that a disruption affecting this operator could have far-reaching effects into other sectors and over national borders. The potential pan-European implications of disruptions call for action at EU level. In addition, diverging national rules result in a direct negative effect on the functioning of the internal market. As the impact assessment has demonstrated, many Member States and industry stakeholders see a need for a more common and coordinated European approach aimed at ensuring that entities are sufficiently resilient in the face of different risks that, while somewhat different from one Member State to another, create many common challenges that cannot be addressed through national measures or by individual operators alone.

- **Proportionality**

The proposal is proportionate in relation to the stated overarching objective of the initiative. While the obligations on Member States and critical entities may in certain cases entail some additional administrative burden, e.g. where Member States need to develop a national strategy or where critical entities must implement certain technical and organisational measures, these are anticipated to be generally limited in nature. In this regard, it should be noted that many entities have already taken some security measures to protect their infrastructures and ensure business continuity.

In some cases, however, achieving compliance with the directive may require more substantial investments. Even in such cases, though, these investments are justified insofar as they would contribute to enhanced operator-level and systemic resilience as well as a more coherent approach and an increased ability to provide reliable services across the Union. Furthermore, any additional burden resulting from the directive is expected to be far exceeded by the costs associated with having to manage and recover from major disruptions that jeopardise the uninterrupted provision of services relating to vital societal functions and the economic well-being of operators, individual Member States, the Union and its citizens more generally.

- **Choice of the instrument**

The proposal takes the form of a directive aimed at ensuring a more common approach to the resilience of critical entities in a number of sectors across the Union. The proposal sets out specific obligations on competent authorities to identify critical entities on the basis of

common criteria and the outcomes of the risk assessment. By way of a directive, it is possible to ensure that Member States apply a uniform approach in identifying critical entities, while at the same time accounting for specificities at national level, including varying levels of risk exposure and interdependencies between sectors and over borders.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Ex-post evaluations/fitness checks of existing legislation**

The European Critical Infrastructure (ECI) Directive was in 2019 subject to an evaluation aimed at assessing the implementation of the directive in terms of its relevance, coherence, effectiveness, efficiency, EU added value and sustainability.[12]

The evaluation found that the context has changed considerably since the directive entered into force. In view of these changes, the directive was found to have only partial relevance. While the evaluation found that the directive was generally consistent with relevant European sectoral legislation and policy at international level, it was seen to be only partially effective due to the generality of some of its provisions. The directive was found to have generated EU added value insofar as it achieved results (i.e. a common framework for the protection of ECIs) that neither national nor other European initiatives could otherwise have achieved without initiating much longer, costlier and less well-defined processes. That being said, certain provisions were found to have had limited added value for many Member States.

With regard to sustainability, certain effects generated by the directive (e.g. cross-border discussions, reporting requirements) were expected to cease were the directive to be repealed and not replaced. The evaluation found that there is continued support on the part of Member States for EU involvement in efforts to strengthen critical infrastructure resilience, and that there is some concern that the outright repeal of the directive might have negative effects in this area, and specifically on protection of designated ECIs. Member States were keen to ensure that the Union's engagement in the field continues to respect the principle of subsidiarity, supports measures at national level, and facilitates cross-border cooperation, including with third countries.

- **Stakeholder consultations**

In developing this proposal, the Commission has consulted a wide variety of stakeholders, including: European Union Institutions and agencies; international organisations; Member State authorities; private entities, including individual operators and national and European industry associations representing operators in many different sectors; experts and expert networks, including the European Reference Network for Critical Infrastructure Protection (ERNCIP); members of academia; non-governmental organisations; and members of the public.

Stakeholders were consulted through a variety of means, including: a public feedback opportunity regarding the Inception Impact Assessment for this proposal; consultative seminars; targeted questionnaires; bilateral exchanges; and a public consultation (to support the 2019 evaluation of the ECI Directive). Moreover, the external contractor responsible for the feasibility study that supported the development of the impact assessment involved

[12] SWD(2019) 310.

consultations with many stakeholders through, e.g. an online survey, a written questionnaire, one-on-one interviews, and virtual 'field visits' in 10 Member States.

These consultations allowed the Commission to explore the effectiveness, efficiency, relevance, coherence and EU added value of the existing framework for critical infrastructure resilience (i.e. the baseline situation), what problems it has generated, different policy options that might be considered in addressing these problems, and the specific impacts that these options might be expected to have. Generally speaking, the consultations pointed to a number of areas where there was overall consensus among stakeholders, not least that the existing EU framework on critical infrastructure resilience should be revamped in light of growing cross-sectoral interdependencies and a shifting threat landscape.

Specifically, stakeholders were in general in agreement that any new approach should consist of a combination of binding and non-binding measures, focus on resilience rather than asset-centric protection, and provide a more obvious link between measures aimed at enhancing cyber- and non-cyber-related resilience. Furthermore, they supported an approach that accounts for provisions in existing sectoral legislation, encompasses at least those sectors covered by the current NIS Directive, and more uniform obligations on critical entities at national level, which in turn should be able to exercise sufficient security scrutiny of personnel with access to sensitive facilities/information. Additionally, stakeholders suggested that any new approach should create opportunities for Member States to carry out enhanced oversight over the activities of critical entities, but also ensure that critical entities of pan-European significance are identified and sufficiently resilient. Finally, they argued for more EU funding and support to, e.g. the implementation of any new instrument, capacity-building at national level, and public-private coordination/cooperation and the sharing of good practice, knowledge and expertise at different levels. The proposal at hand contains provisions that generally correspond to the views and preferences expressed by stakeholders.

- **Collection and use of expertise**

As mentioned in the preceding section, the Commission has drawn on external expertise in the context of consultations with, e.g. independent experts, expert networks and members of academia, in developing the proposal at hand.

- **Impact assessment**

The impact assessment that supported the development of this initiative explored different policy options to address the general and specific problems described earlier. Besides the baseline situation, which would entail no change over the current situation, these options included:

– Option 1: The retention of the existing ECI Directive, accompanied by voluntary measures within the context of the existing EPCIP programme;

– Option 2: The revision of the existing ECI Directive to cover the same sectors as the existing NIS Directive and to focus more on resilience. The new ECI directive would entail changes to the existing cross-border ECI designation process, including new designation criteria, and new requirements on Member States and operators;

– Option 3: The replacement of the existing ECI Directive with a new instrument aimed at enhancing the resilience of critical entities in the sectors considered as essential by the proposed NIS 2 Directive. This option would set out minimum requirements for Member States and critical entities identified under the new

framework. A procedure for the identification of critical entities offering services to or in several if not all EU Member States would be provided. The implementation of the legislation would be supported by a dedicated knowledge hub within the Commission.

– Option 4: The replacement of the existing ECI Directive with a new instrument aimed at enhancing the resilience of critical entities in the sectors considered as essential by the proposed NIS 2 Directive, as well as a more substantial role for the Commission in identifying critical entities and the creation of a dedicated EU Agency responsible for critical infrastructure resilience (which would assume the roles and responsibilities assigned to the knowledge hub proposed in previous option).

In light of the various economic, social and environmental impacts associated with each of the options, but also their value in terms of effectiveness, efficiency and proportionality, the impact assessment found that the preferred option was Option 3. While Options 1 and 2 would not deliver the changes needed to address the problem, Option 3 would result in a harmonised and more comprehensive resilience framework that would also be aligned with and account for existing Union law in related fields. Option 3 was also found to be proportionate and to appear politically feasible as it aligns with the statements of the Council and Parliament regarding the need for Union action in this area. Furthermore, this option was found to be likely to ensure flexibility and offer a future-proof framework that would allow critical entities to respond to different risks over time. Finally, the impact assessment found that this option would be complementary to existing sectoral and cross-sectoral frameworks and instruments. For instance, this option makes allowances for when designated entities meet certain obligations contained in this new instrument through obligations in existing ones, in which case they would not be required to take further action. On the other hand, they would be expected to take certain measures where existing instruments do not cover the matter or are limited to only certain types of risks or measures.

The impact assessment was subject to scrutiny by the Regulatory Scrutiny Board, which issued a positive opinion with reservations on 20 November 2020. The Board pointed to a number of elements of the impact assessment that should be addressed. Specifically, the Board requested further clarification concerning the risks related to critical infrastructure and the cross-border dimension, the link between the initiative and the ongoing revision of the NIS Directive, and the relationship between the preferred policy option and other pieces of sectoral legislation. Furthermore, the Board saw the need for further justification for expanding the sectoral scope of the instrument, and requested additional information concerning the criteria for selecting critical entities. Finally, as regards proportionality, the Board sought additional clarification as to how the preferred option would lead to better national responses to cross-border risks. These and other more detailed comments provided by the Board have been addressed in the final version of the impact assessment, which, for instance, describes in more detail the cross-border risks to critical infrastructures and the relationship between this proposal and the proposal for the NIS 2 directive. The Board's comments have also been accounted for in the proposed directive that follows.

- **Regulatory fitness and simplification**

In line with the Commission's Regulatory Fitness and Performance Programme (REFIT), all initiatives aimed at changing existing EU legislation should seek to simplify and deliver stated policy objectives more efficiently. The findings of the impact assessment suggest that the proposal should reduce the overall burden on Member States. Closer alignment with the

services-oriented approach of the current NIS Directive is likely to lead to reduced compliance costs over time. For instance, the burdensome cross-border identification and designation process contained in the existing ECI Directive would be replaced with a risk-based procedure at national level aimed only at identifying critical entities subject to various obligations. On the basis of the risk assessment, Member States would identify critical entities, most of which are already designated operators of essential services per the current NIS Directive.

Furthermore, by taking measures to enhance their resilience, critical entities will be less likely to experience disruptions. Thus, the likelihood for disruptive incidents affecting negatively the provision of essential services in individual Member States and across Europe would be reduced. This, together with the positive effects resulting from harmonising at Union level diverging national rules, would have a positive impact on businesses, including micro-enterprises and small and medium enterprises, the overall health of the Union economy and the reliable functioning of the internal market.

- **Fundamental rights**

The proposed legislation is intended to enhance the resilience of critical entities providing various forms of essential services, whilst eliminating regulatory obstacles to their ability to provide their services across the Union. In so doing, the overall risk for disruptions at both societal and individual level would be reduced and burdens would be reduced. That would contribute to ensuring a higher level of public security whilst also positively affecting the freedom of companies to conduct business, as well as many other economic operators reliant on the provision of essential services, ultimately benefitting consumers. The proposal's provisions aimed at ensuring effective employee security management will normally involve the processing of personal data. This is justified by the need to carry out background checks on specific categories of personnel. Moreover, any such processing of personal data will always be subject to compliance with Union rules on the protection of personal data, including the General Data Protection Regulation.[13]

4. BUDGETARY IMPLICATIONS

The proposed directive has implications for the Union budget. The total financial resources necessary to support the implementation of this proposal are estimated to be EUR 42.9 million for the period 2021-2027, of which EUR 5.1 million is administrative expenditure. These costs can be broken down as follows:

– Support activities by the Commission–including staffing, projects, studies and support activities;

– Advisory missions organised by the Commission;

– Regular meetings of the Critical Entity Resilience Group, Comitology Committee and other meetings.

More detailed information is available in the Legislative Financial Statement that accompanies this proposal.

[13] 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.

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

The implementation of the proposed directive will be reviewed by four years and a half after its entry into force, after which the Commission will submit a report to the European Parliament and to the Council. This report will assess the extent to which the Member States have taken the necessary measures to comply with the directive. A report assessing the impact and added value of the directive will be submitted by the Commission to the European Parliament and to the Council by six years after the entry info force of the directive.

- **Detailed explanation of the specific provisions of the proposal**

Subject matter, scope and definitions (Articles 1-2)

Article 1 sets out the subject matter and scope of the directive, which lays down obligations for Member States to take certain measures aimed at ensuring the provision in the internal market of services essential for the maintenance of vital societal functions or economic activities, in particular to identify critical entities and to enable them to meet specific obligations aimed at enhancing their resilience and improving their ability to provide those services in the internal market. The directive also establishes rules on supervision and enforcement of critical entities and the specific oversight of critical entities considered to be of particular European significance. Article 1 also explains the relationship between the directive and other relevant acts of Union law, and the conditions under which information that is confidential pursuant to Union and national rules shall be exchanged with the Commission and other relevant authorities. Article 2 provides a list of definitions that apply.

National frameworks on the resilience of critical entities (Articles 3-9)

Article 3 states that Member States shall adopt a strategy for reinforcing the resilience of critical entities, describes the elements that it should contain, explains that it should be updated regularly and where necessary, and stipulates that Member States shall communicate their strategies and any updates of their strategies to the Commission. Article 4 states that competent authorities shall establish a list of essential services and carry out regularly an assessment of all relevant risks that may affect the provision of those essential services with a view to identifying critical entities. This assessment shall account for the risk assessments carried out in accordance with other relevant acts of Union law, the risks arising from the dependencies between specific sectors, and available information on incidents. Member States shall ensure that relevant elements of the risk assessment are made available to critical entities, and that data on the types of risks identified and the outcomes of their risk assessments is made regularly available to the Commission.

Article 5 states that Member States shall identify critical entities in specific sectors and sub-sectors. The identification process should account for the outcomes of the risk assessment and apply specific criteria. Member States shall establish a list of critical entities, which shall be updated where necessary and regularly. Critical entities shall be duly notified of their identification and the obligations that this entails. Competent authorities responsible for the implementation of the directive shall notify the competent authorities responsible for the implementation of the NIS 2 Directive of the identification of critical entities. Where an entity has been identified as critical by two or more Member States, the Member States shall engage in consultation with each other with a view to reduce the burden on the critical entity. Where critical entities provide services to or in more than one third of Member States, the Member State concerned shall notify to the Commission the identities of those critical entities.

Article 6 defines the term 'significant disruptive effect' as referred to in Article 5(2), and requires that Member States submit to the Commission certain forms of information pertaining to the critical entities that they identify and how they were identified. Article 6 also empowers the Commission, after consultation of the Critical Entities Resilience Group, to adopt relevant guidelines.

Article 7 establishes that Member States should identify entities in the banking, financial market infrastructure and digital infrastructure sectors that are to be treated as equivalent to critical entities for the purposes of chapter II only. These entities should be notified of their identification.

Article 8 stipulates that each Member State shall designate and ensure that adequate resources are provided to one or more competent authorities responsible for the correct application of the directive at national level as well as a single point of contact tasked with ensuring cross-border cooperation. The single point of contact shall provide a summary report on incident notifications to the Commission on a regular basis. Article 8 requires that competent authorities responsible for the application of the directive cooperate with other relevant national authorities, including competent authorities designated under the NIS 2 Directive. Article 9 stipulates that Member States shall provide support to critical entities in ensuring their resilience, and shall facilitiate cooperation and the voluntary exchange of information and good practices between competent authorities and critical entities.

Resilience of critical entities (Articles 10-13)

Article 10 states that critical entities shall regularly assess all relevant risks on the basis of national risk assessments and other relevant sources of information. Article 11 stipulates that critical entities shall take appropriate and proportionate technical and organisational measures to ensure their resilience, and shall ensure that these measures are described in a resilience plan or equivalent document or documents. Member States may request that the Commission organise advisory missions to provide advice to critical entities in meeting their obligations. Article 11 also empowers the Commission, where necessary, to adopt delegated and implementing acts.

Article 12 states that Member States shall ensure that critical entities may submit requests for background checks for persons who fall or might come to fall within certain specific categories of personnel, and that these requests are assessed expeditiously by the authorities responsible for carrying out such background checks. The article describes the purpose, scope and contents of the background checks, all of which shall comply with the General Data Protection Regulation.

Article 13 states that Member States shall ensure that critical entities notify the competent authority of incidents that significantly disrupt or have the potential to significantly disrupt their operations. Competent authorities in turn shall provide the notifying critical entity with relevant follow-up information. Via the single point of contact, competent authorities shall also inform the single points of contact in other affected Member States in the event that the incident has, or may have, cross-border impacts in one or more other Member States.

Specific oversight over critical entities of particular European significance (Articles 14-15)

Article 14 defines critical entities of particular European significance as entities that have been identifed as critical entities and that provide essential services to or in more than one third of Member States. Upon receiving notification pursuant to Article 5(6), the Commission

shall inform the entity concerned that it is considered a critical entity of particular European signficance, the obligations that this entails and the date from which those obligations begin to apply. Article 15 describes the specific oversight arrangements applicable to critical entities of particular European significance, which include, upon request, that host Member States provide the Commission and Critical Entities Resilience Group with information concerning the risk assessment pursuant to Article 10 and the measures taken in accordance with Article 11, as well as any supervisory or enforcement actions. Article 15 also stipulates that the Commission may organise advisory missions to assess the measures put in place by specific critical entities of particular European significance. On the basis of an analysis of the advisory mission's findings by the Critical Entities Resilience Group, the Commission shall communicate its views to the Member State where the infrastructure of the entity is located on whether that entity complies with its obligations and, where appropriate, which measures could be taken to improve the resilience of the entity. The article describes the composition, organisation and funding of the advisory missions. It also stipulates that the Commission shall adopt an implementing act laying down rules on the procedural arrangements for the conduct and reports of advisory missions.

Cooperation and reporting (Articles 16-17)

Article 16 describes the role and tasks of the Critical Entities Resilience Group, which shall be composed of representatives of the Member States and the Commission. It shall support the Commission and facilitate strategic cooperation and the exchance of information. The article explains that the Commission may adopt implementing acts laying down procedural arrangements necessary for the functioning of the Critical Entities Resilience Group. Article 17 stipulates that the Commission shall, where appropriate, support Member States and critical entities in complying with their obligations under the directive, and complement Member State activities referred to in Article 9.

Supervision and enforcement (Articles 18-19)

Article 18 states that Member States have certain powers, means and responsibilities in ensuring the implementation and enforcement of the directive. Member States shall ensure that, when a competent authority assesses the compliance of a critical entity, it shall inform the competent authorities of the Member State concerned designated under the NIS 2 Directive and may request these authorities to assess the cybersecurity of such entity, and should cooperate and exchange information for this purpose. Article 19 states that, in accordance with long-standing practice, Member States are to lay down the rules on penalties applicable to infringements and to take all measures necessary to ensure that they are implemented.

Final provisions (Articles 20-26)

Article 20 states that the Commission shall be assisted by a committee within the meaning of Regulation (EU) 182/2011. This is a standard article. Article 21 confers to the Commission the power to adopt delegated acts subject to conditions laid down in the article. This, too, is a standard article. Article 22 states that the Commission shall submit a report to the European Parliament and to the Council assessing the extent to which the Member States have taken the necessary measures to comply with the directive. A report assessing the impact and added value of the directive and whether the scope of the directive should be extended to other sectors or subsectors, including the food production, processing and distribution sector, must be submitted regularly to the European Parliament and to the Council.

Article 23 states that Directive 2008/114/EC is repealed with effect from the date of entry into application of the directive. Article 24 states that Member States shall adopt and publish, within the set time period, the laws, regulations and administrative provisions necessary to comply with the directive, and inform the Commission thereof. The text of the main provisions of national law which they adopt in the field covered by this directive shall be communicated to the Commission. Article 25 states that the directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*. Article 26 states that the directive is addressed to the Member States.

2020/0365 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the resilience of critical entities

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Economic and Social Committee[14],

Having regard to the opinion of the Committee of the Regions[15],

Acting in accordance with the ordinary legislative procedure[16],

Whereas:

(1) Council Directive 2008/114/EC[17] provides for a procedure for designating European critical infrastructures in the energy and transport sectors, the disruption or destruction of which would have significant cross-border impact on at least two Member States. That Directive focused exclusively on the protection of such infrastructures. However, the evaluation of Directive 2008/114/EC conducted in 2019[18] 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 the resilience of critical entities, that is, their ability to mitigate, absorb, accommodate to and recover from incidents that have the potential to disrupt the operations of the critical entity.

(2) Despite existing measures at Union[19] and national level aimed at supporting the protection of critical infrastructures in the Union, the entities operating those infrastructures are not adequately equipped to address current and anticipated future risks to their operations that may result in disruptions of the provision of services that are essential for the performance of vital societal functions or economic activities. This is due to a dynamic threat landscape with an evolving terrorist threat and growing interdependencies between infrastructures and sectors, as well as an increased physical risk due to natural disasters and climate change, which increases the frequency and

---

14 OJ C , , p. .

15 OJ C […], […], p. […].

16 Position of the European Parliament […] and of the Council […].

17 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).

18 SWD(2019) 308.

19 European Programme for Critical Infrastructure Protection (EPCIP).

scale of extreme weather events and brings long-term changes in average climate that can reduce the capacity and efficiency of certain infrastructure types if resilience or climate adaptation measures are not in place. Moreover, relevant sectors and types of entities are not recognised consistently as critical in all Member States.

(3) Those growing interdependencies are the result of an increasingly cross-border and interdependent network of service provision using key infrastructures across the Union in the sectors of energy, transport, banking, financial market infrastructure, digital infrastructure, drinking and waste water, health, certain aspects of public administration, as well as space in as far as the provision of certain services depending on ground-based infrastructures that are owned, managed and operated either by Member States or by private parties is concerned, therefore not covering infrastructures owned, managed or operated by or on behalf of the Union as part of its space programmes. These interdependencies mean that any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the internal market. The COVID-19 pandemic has shown the vulnerability of our increasingly interdependent societies in the face of low-probability risks.

(4) The entities involved in the provision of essential services are increasingly subject to diverging requirements imposed under the laws of the Member States. The fact that some Member States have less stringent security requirements on these entities not only risks impacting negatively on the maintenance of vital societal functions or economic activities across the Union, it also leads to obstacles to the proper functioning of the internal market. Similar types of entities are considered as critical in some Member States but not in others, and those which are identified as critical are subject to divergent requirements in different Member States. This results in additional and unnecessary administrative burdens for companies operating across borders, notably for companies active in Member States with more stringent requirements.

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

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

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

(8) Given the importance of cybersecurity for the resilience of critical entities and in the interest of consistency, a coherent approach between this Directive and Directive (EU)

XX/YY of the European Parliament and of the Council[20] [Proposed Directive on measures for a high common level of cybersecurity across the Union; (hereafter "NIS 2 Directive")] is necessary wherever possible. In view of the higher frequency and particular characteristics of cyber risks, the NIS 2 Directive imposes comprehensive requirements on a large set of entities to ensure their cybersecurity. Given that cybersecurity is addressed sufficiently in the NIS 2 Directive, the matters covered by it should be excluded from the scope of this Directive, without prejudice to the particular regime for entities in the digital infrastructure sector.

(9) Where provisions of other acts of Union law require critical entities to assess relevant risks, take measures to ensure their resilience or notify incidents, and those requirements are at least equivalent to the corresponding obligations laid down in this Directive, the relevant provisions of this Directive should not apply, so as to avoid duplication and unnecessary burdens. In that case, the relevant provisions of such other acts should apply. Where the relevant provisions of this Directive do not apply, its provisions on supervision and enforcement should not be applicable either. Member States should nevertheless include all the sectors listed in the Annex in their strategy for reinforcing the resilience of critical entities, the risk assessment and the support measures pursuant to Chapter II and be able to identify critical entities in those sectors where the applicable conditions have been met, taking into account the particular regime for entities in the banking, financial market infrastructure and digital infrastructure sector.

(10) In view of ensuring a comprehensive approach to the resilience of critical entities, each Member State should have a strategy setting out objectives and policy measures to be implemented. To achieve this, Member States should ensure that their cybersecurity strategies provide for a policy framework for enhanced coordination between the competent authority under this Directive and the NIS 2 Directive in the context of information sharing on incidents and cyber threats and the exercise of supervisory tasks.

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

(12) In order to ensure that all relevant entities are subject to those requirements and to reduce divergences in this respect, it is important to lay down harmonised rules allowing for a consistent identification of critical entities across the Union, while also allowing Member States to reflect national specificities. Therefore, criteria to identify critical entities should be laid down. In the interest of effectiveness, efficiency,

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

consistency and legal certainty, appropriate rules should also be set on notification and cooperation relating to, as well as the legal consequences of, such identification. In order to enable the Commission to assess the correct application of this Directive, Member States should submit to the Commission, in a manner that is as detailed and specific as possible, relevant information and, in any event, the list of essential services, the number of critical entities identified for each sector and subsector referred to in the Annex and the essential service or services that each entity provides and any thresholds applied.

(13) Criteria should also be established to determine the significance of a disruptive effect produced by such incidents. Those criteria should build on the criteria provided in Directive (EU) 2016/1148 of the European Parliament and of the Council[21] in order to capitalise on the efforts carried out by Member States to identify those operators and the experience gained in this regard.

(14) Entities pertaining to the digital infrastructure sector are in essence based on network and information systems and fall within the scope of the NIS 2 Directive, which addresses the physical security of such systems as part of their cybersecurity risk management and reporting obligations. Since those matters are covered by the NIS 2 Directive, the obligations of this Directive do not apply to such entities. However, considering the importance of the services provided by entities in the digital infrastructure sector for the provision of other essential services, Member States should identify, based on the criteria and using the procedure provided for in this Directive *mutatis mutandis*, entities pertaining to the digital infrastructure sector that should be treated as equivalent to critical entities for the purposes of Chapter II only, including the provision on Member States' support in enhancing the resilence of these entities. Consequently, such entities should not be subject to the obligations laid down in Chapters III to VI. Since the obligations for critical entities laid down in Chapter II to provide certain information to the competent authorities relate to the application of Chapters III and IV, those entities should not be subject to those obligations either.

(15) The EU financial services acquis establishes comprehensive requirements on financial entities to manage all risks they face, including operational risks and ensure business continuity. This includes Regulation (EU) No 648/2012 of the European Parliament and of the Council[22], Directive 2014/65/EU of the European Parliament and of the Council[23] and Regulation (EU) No 600/2014 of the European Parliament and of the Council [24] as well as Regulation (EU) No 575/2013 of the European Parliament and of the Council[25] and Directive 2013/36/EU of the European Parliament and of the

---

21 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).

22 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).

23 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).

24 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).

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

Council[26]. The Commission has recently proposed to complement this framework with Regulation XX/YYYY of the European Parliament and of the Council [proposed Regulation on digital operational resilience for the financial sector (hereafter "DORA Regulation")[27]], which lays down requirements for financial firms to manage ICT risks, including the protection of physical ICT infrastructures. Since the resilience of entities listed in points 3 and 4 of the Annex is comprehensively covered by the EU financial services acquis, those entities should also be treated as equivalent to critical entities for the purposes of Chapter II of this Directive only. To ensure a consistent application of the operational risk and digital resilience rules in the financial sector, Member States' support to enhancing the overall resilience of financial entities equivalent to critical entities should be ensured by the authorities designated pursuant to Article 41 of [DORA Regulation], and subject to the procedures set out in that legislation in a fully harmonised manner.

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

(17) In order to facilitate cross-border cooperation and communication and to enable the effective implementation of this Directive, each Member State should, without prejudice to sector-specific Union legal requirements, designate, within one of the authorities it designated as competent authority under this Directive, a single point of contact responsible for coordinating issues related to the resilience of critical entities and cross-border cooperation at Union level in this regard.

(18) Given that under the NIS 2 Directive entities identified as critical entities, as well as identified entities in the digital infrastructure sector that are to be treated as equivalent under the present Directive are subject to the cybersecurity requirements of the NIS 2 Directive, the competent authorities designated under the two Directives should cooperate, particularly in relation to cybersecurity risks and incidents affecting those entities.

(19) Member States should support critical entities in strengthening their resilience, in compliance with their obligations under this Directive, without prejudice to the entities' own legal responsibility to ensure such compliance. Member States could in particular develop guidance materials and methodologies, support the organisation of exercises to test their resilience and provide training to personnel of critical entities. Moreover, given the interdependencies between entities and sectors, Member States

---

[26] 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).

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

should establish information sharing tools to support voluntary information sharing between critical entities, without prejudice to the application of competition rules laid down in the Treaty on the Functioning of the European Union.

(20) In order to be able to ensure their resilience, critical entities should have a comprehensive understanding of all relevant risks to which they are exposed and analyse those risks. To that aim, they should carry out risks assessments, whenever necessary in view of their particular circumstances and the evolution of those risks, yet in any event every four years. The risk assessments by critical entities should be based on the risk assessment carried out by Member States.

(21) Critical entities should take organisational and technical measures that are appropriate and proportionate to the risks they face so as to prevent, resist, mitigate, absorb, accommodate to and recover from an incident. Although critical entities should take measures on all points specified in this Directive, the details and extent of the measures should reflect the different risks that each entity has identified as part of its risk assessment and the specificities of such entity in an appropriate and proportionate way.

(22) In the interest of effectiveness and accountability, critical entities should describe those measures, with a level of detail to sufficiently achieve those aims, having regard to the risks identified, in a resilience plan or in a document or documents that are equivalent to a resilience plan, and apply that plan in practice. Such equivalent document or documents may be drawn up in accordance with requirements and standards developed in the context of international agreements on physical protection to which Member States are parties, including the Convention on the physical protection of nuclear material and nuclear facilities, as appropriate.

(23) Regulation (EC) No 300/2008 of the European Parliament and of the Council[28], Regulation (EC) No 725/2004 of the European Parliament and of the Council[29] and Directive 2005/65/EC of the European Parliament and of the Council[30] establish requirements applicable to entities in the aviation and maritime transport sectors to prevent incidents caused by unlawful acts and to resist and mitigate the consequences of such incidents. While the measures required in this Directive are broader in terms of risks addressed and types of measures to be taken, critical entities in those sectors should reflect in their resilience plan or equivalent documents the measures taken pursuant to those other Union acts. Moreover, when implementing resilience measures under this Directive, critical entities may consider referring to non-binding guidelines and good practices documents developed under sectorial workstreams, such as the EU Rail Passenger Security Platform[31].

(24) The risk of employees of critical entities misusing for instance their access rights within the entity's organisation to harm and cause damage is of increasing concern. That risk is exacerbated by the growing phenomenon of radicalisation leading to

---

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

29 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.).

30 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).

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

violent extremism and terrorism. It is therefore necessary to enable critical entities to request background checks on persons falling within specific categories of its personnel and to ensure that those requests are assessed expeditiously by the relevant authorities, in accordance with the applicable rules of Union and national law, including on the protection of personal data.

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

(26) While critical entities generally operate as part of an increasingly interconnected network of service provision and infrastructures and often provide essential services in more than one Member State, some of those entities are of particular significance for the Union because they provide essential services to a large number of Member States, and therefore require specific oversight at Union level. Rules on the specific oversight in respect of such critical entities of particular European significance should therefore be established. Those rules are without prejudice to the rules on supervision and enforcement set out in this Directive.

(27) Where any Member State considers that additional information is necessary to be able to advise a critical entity in meeting its obligations under Chapter III or to assess the compliance of a critical entity of particular European significance with those obligations, in agreement with the Member State where the infrastructure of that entity is located, the Commission should organise an advisory mission to assess the measures put in place by that entity. In order to ensure that such advisory missions are carried out properly, complementary rules should be established, notably on their organisation and conduct, the follow-up to be given and the obligations for the critical entities of particular European significance concerned. The advisory missions should, without prejudice to the need for the Member State where the advisory mission is conducted and the entity concerned to comply with the rules of this Directive, be conducted subject to the detailed rules of the law of that Member State, for instance on the precise conditions to be fulfilled to obtain access to relevant premises or documents and on judicial redress. Specific expertise required for such missions could, where relevant, be requested through the Emergency Response Coordination Centre.

(28) In order to support the Commission and facilitate strategic cooperation and the exchange of information, including best practices, on issues relating to this Directive, a Critical Entities Resilience Group, which is a Commission expert group, should be established. Member States should endeavour to ensure effective and efficient cooperation of the designated representatives of their competent authorities in the Critical Entities Resilience Group. The group should begin to perform its tasks from six months after the entry into force of this Directive, so as to provide additional means for appropriate cooperation during the transposition period of this Directive.

(29) In order to achieve the objectives of this Directive, and without prejudice to the legal responsibility of Member States and critical entities to ensure compliance with their respective obligations set out therein, the Commission should, where it considers it appropriate, undertake certain supporting activities aimed at facilitating compliance with those obligations. When providing support to Member States and critical entities in the implementation of obligations under this Directive, the Commission should build on existing structures and tools, such as those under the Union Civil Protection mechanism and the European Reference Network for Critical Infrastructure Protection.

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

(31) In order to take into account new risks, technological developments or specificities of one or more of the sectors, the power to adopt acts in accordance with Article 290 Treaty on the Functioning of the European Union should be delegated to the Commission to supplement the resilience measures critical entities are to take by further specifying some or all of those measures. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[32]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(32) In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[33].

---

32 OJ L 123, 12.5.2016, p. 1.

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

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

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

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I
SUBJECT MATTER , SCOPE AND DEFINITIONS

Article 1
Subject matter and scope

1. This Directive:

   (a) lays down obligations for Member States to take certain measures aimed at ensuring the provision in the internal market of services essential for the maintenance of vital societal functions or economic activities, in particular to identify critical entities and entities to be treated as equivalent in certain respects, and to enable them to meet their obligations;

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

   (c) establishes rules on supervision and enforcement of critical entities, and specific oversight of critical entities considered to be of particular European significance.

2. This Directive shall not apply to matters covered by Directive (EU) XX/YY [proposed Directive on measures for a high common level of cybersecurity across the Union; ('NIS 2 Directive')], without prejudice to Article 7.

3. Where provisions of sector-specific acts of Union law require critical entities to take measures as set out in Chapter III, and where those requirements are at least equivalent to the obligations laid down in this Directive, the relevant provisions of this Directive shall not apply, including the provisions on supervision and enforcement laid down in Chapter VI.

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

Article 2
Definitions

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

(1) "critical entity" means a public or private entity of a type referred to in the Annex, which has been identified as such by a Member State in accordance with Article 5;

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

(3) "incident" means any event having the potential to disrupt, or that disrupts, the operations of the critical entity;

(4) "infrastructure" means an asset, system or part thereof, which is necessary for the delivery of an essential service;

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

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

(7) "risk assessment" means a methodology to determine the nature and extent of a risk by analysing potential threats and hazards and evaluating existing conditions of vulnerability that could disrupt the operations of the critical entity.

CHAPTER II
NATIONAL FRAMEWORKS ON THE RESILIENCE OF CRITICAL ENTITIES

Article 3
Strategy on the resilience of critical entities

1. Each Member State shall adopt by [three years after entry into force of this Directive] a strategy for reinforcing the resilience of critical entities. This strategy shall set out strategic objectives and policy measures with a view to achieving and maintaining a high level of resilience on the part of those critical entities and covering at least the sectors referred to in the Annex.

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

   (a) strategic objectives and priorities for the purposes of enhancing the overall resilience of critical entities taking into account cross-border and cross-sectoral 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 national risk assessment, the identification of critical entities and of entities equivalent to critical entities, and the measures to support critical entities taken in accordance with this Chapter;

   (d) a policy framework for enhanced coordination between the competent authorities designated pursuant to Article 8 of this Directive and pursuant to

[the NIS 2 Directive] for the purposes of information sharing on incidents and cyber threats and the exercise of supervisory tasks.

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

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

Article 4
Risk assessment by Member States

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

   The risk assessment shall account for all relevant natural and man-made risks, including accidents, natural disasters, public health emergencies, antagonistic threats, including terrorist offences pursuant to Directive (EU) 2017/541 of the European Parliament and of the Council[34].

2. In carrying out the risk assessment, Member States shall take into account as a minimum:

   (a) the general risk assessment carried out pursuant to Article 6(1) of Decision No 1313/2013/EU of the European Parliament and of the Council[35];

   (b) other relevant risk assessments, carried out in accordance with the requirements of the relevant sector-specific acts of Union law, including Regulation (EU) 2019/941 of the European Parliament and of the Council[36] and Regulation (EU) 2017/1938 of the European Parliament and of the Council[37];

   (c) any risks arising from the dependencies between the sectors referred to in the Annex, including from other Member States and third countries, and the impact that a disruption in one sector may have on other sectors;

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

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

---

34 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).

35 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).

36 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).

37 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).

3. Member States shall make the relevant elements of the risk assessment referred to in paragraph 1 available to the critical entities that they identified in accordance with Article 5 in order to assist those critical entities in carrying out their risk assessment, pursuant to Article 10, and in taking measures to ensure their resilience pursuant to Article 11.

4. Each Member State shall provide the Commission with data on the types of risks identified and the outcomes of the risk assessments, per sector and sub-sector referred to in the Annex, by [three years after entry into force of this Directive] and subsequently where necessary and at least every four years.

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

Article 5
Identification of critical entities

1. By [three years and three months after entry into force of this Directive] Member States shall identify for each sector and subsector referred to in the Annex, other than points 3, 4 and 8 thereof, the critical entities.

2. When identifying critical entities pursuant to paragraph 1, Member States shall take into account the outcomes of the risk assessment pursuant to Article 4 and apply the following criteria:

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

   (b) (the provision of that service depends on infrastructure located in the Member State; and

   (c) an incident would have significant disruptive effects on the provision of the service or of other essential services in the sectors referred to in the Annex that depend on the service.

3. Each Member State shall establish a list of the critical entities identified and ensure that those critical entities are notified of their identification as critical entities within one month of that identification, informing them of their obligations pursuant to Chapters II and III and the date from which the provisions of those Chapters apply to them.

   For the critical entities concerned, the provisions of this Chapter shall apply from the date of the notification and the provisions of Chapter III shall apply from six months after that date.

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

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

engage in consultation with each other with a view to reduce the burden on the critical entity in regard to the obligations pursuant to Chapter III.

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

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

Where those updates lead to the identification of additional critical entities, paragraphs 3, 4, 5 and 6 shall apply. In addition, Member States shall ensure that entities that are no longer identified as critical entities pursuant to any such update are notified thereof and are informed that they are no longer subject to the obligations pursuant to Chapter III as from the reception of that information.

Article 6
Significant disruptive effect

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

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

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

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

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

(e) the geographic area that could be affected by an incident, including any cross-border impacts;

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

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

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

(b) the number of critical entities identified for each sector and subsector referred to in the Annex and the service or services referred to in Article 4(1) that each entity provides;

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

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

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

Article 7

Entities equivalent to critical entities under this Chapter

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

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

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

Article 8

Competent authorities and single point of contact

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

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

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

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

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

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

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

7. Each Member State shall notify the Commission of the designation of the competent authority and single point of contact within three months from that designation, including their precise tasks and responsibilities under this Directive, their contact details and any subsequent change thereto. Each Member State shall make public its designation of the competent authority and single point of contact.

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

Article 9
Member States' support to critical entities

1. Member States shall support critical entities in enhancing their resilience. That support may include developing guidance materials and methodologies, supporting the organisation of exercises to test their resilience and providing training to personnel of critical entities.

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

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

CHAPTER III
RESILIENCE OF CRITICAL ENTITIES

Article 10
Risk assessment by critical entities

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

The risk assessment shall account for all relevant risks referred to in Article 4(1) which could lead to the disruption of the provision of essential services. It shall take into account any dependency of other sectors referred to in the Annex on the essential service provided by the critical entity, including in neighbouring Member States and third countries where relevant, and the impact that a disruption of the provision of essential services in one or more of those sectors may have on the essential service provided by the critical entity.

Article 11
Resilience measures of critical entities

1. Member States shall ensure that critical entities take appropriate and proportionate technical and organisational measures to ensure their resilience, including measures necessary to:

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

(b) ensure adequate physical protection of sensitive areas, facilities and other infrastructure, including fencing, barriers, perimeter monitoring tools and routines, as well as detection equipment and access controls;

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

(d) recover from incidents, including business continuity measures and the identification of alternative supply chains;

(e) ensure adequate employee security management, including by setting out categories of personnel exercising critical functions, establishing access rights to sensitive areas, facilities and other infrastructure, and to sensitive information as well as identifying specific categories of personnel in view of Article 12;

(f) raise awareness about the measures referred to in points (a) to (e) among relevant personnel.

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

3. Upon request of the Member State that identified the critical entity and with the agreement of the critical entity concerned, the Commission shall organise advisory missions, in accordance with the arrangements set out in Article 15(4), (5), (7) and (8), to provide advice to the critical entity concerned in meeting its obligations pursuant to Chapter III. The advisory mission shall report its findings to the Commission, that Member State and the critical entity concerned.

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

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

Article 12
Background checks

1. Member States shall ensure that critical entities may submit requests for background checks on persons who fall within certain specific categories of their personnel, including persons being considered for recruitment to positions falling within those categories, and that those requests are assessed expeditiously by the authorities competent to carry out such background checks.

2. In accordance with applicable Union and national law, including Regulation (EU) 2016/679/EU of the European Parliament and of the Council [38], a background check as referred to in paragraph 1 shall:

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

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

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

As regards point (b) of the first subparagraph, Member States shall ensure that their authorities competent to carry out background checks obtain the information on criminal records from other Member States through ECRIS in accordance with the procedures set out in Council Framework Decision 2009/315/JHA, and, where relevant, Regulation (EU) 2019/816 of the European Parliament and of the Council[39]. The central authorities referred to in Article 3 of that Framework Decision and in Article 3(5) of that Regulation shall provide replies to requests for such information within 10 working days from the date the request was received.

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

Article 13
Incident notification

1. Member States shall ensure that critical entities notify without undue delay the competent authority of incidents that significantly disrupt or have the potential to significantly disrupt their operations. Notifications shall include any available information necessary to enable the competent authority to understand the nature, cause and possible consequences of the incident, including so as to determine any cross-border impact of the incident. Such notification shall not make the critical entities subject to increased liability.

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

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

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

[38] OJ L 119, 4.5.2016, p. 1.
[39] OJ L 135, 22.5.2019, p. 1.

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

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

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

4. As soon as possible upon having been notified in accordance with paragraph 1, the competent authority shall provide the critical entity that notified it with relevant information regarding the follow-up of its notification, including information that could support the critical entity's effective response to the incident.

CHAPTER IV
SPECIFIC OVERSIGHT OVER CRITICAL ENTITIES OF PARTICULAR EUROPEAN SIGNIFICANCE

Article 14
Critical entities of particular European significance

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

2. An entity shall be considered a critical entity of particular European significance when it has been identified as a critical entity and it provides essential services to or in more than one third of Member States and has been notified as such to the Commission pursuant to Article 5(1) and (6), respectively.

3. The Commission shall, without undue delay upon receiving the notification pursuant to Article 5(6), notify the entity concerned that it is considered a critical entity of particular European significance, informing that entity of its obligations pursuant to this Chapter and the date from which those obligations apply to it.

The provisions of this Chapter shall apply to the critical entity of particular European significance concerned from the date of receipt of that notification.

Article 15
Specific oversight

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

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

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

3. The advisory mission shall report its findings to the Commission, the Critical Entities Resilience Group and the critical entity of particular European significance concerned within a period of three months after the conclusion of the advisory mission.

   The Critical Entities Resilience Group shall analyse the report and, where necessary, shall advise the Commission on whether the critical entity of particular European significance concerned complies with its obligations pursuant to Chapter III and, where appropriate, which measures could be taken to improve the resilience of that entity.

   The Commission shall, based on that advice, communicate its views to the Member State where the infrastructure of that entity is located, the Critical Entities Resilience Group and that entity on whether that entity complies with its obligations pursuant to Chapter III and, where appropriate, which measures could be taken to improve the resilience of that entity.

   That Member State shall take due account of those views and provide information to the Commission and the Critical Entities Resilience Group on any measures it has taken pursuant to the communication.

4. Each advisory mission shall consist of experts from Member States and of Commission representatives. Member States may propose candidates to be part of an advisory mission. The Commission shall select and appoint the members of each advisory mission according to their professional capacity and ensuring a geographically balanced representation among Member States. The Commission shall bear the costs related to the participation in the advisory mission.

   The Commission shall organise the programme of an advisory mission, in consultation with the members of the specific advisory mission and in agreement with the Member State where the infrastructure of the critical entity or the critical entity of European significance concerned is located.

5. The Commission shall adopt an implementing act laying down rules on the procedural arrangements for the conduct and reports of advisory missions. This implementing act shall be adopted in accordance with the examination procedure referred to in Article 20(2).

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

7. The advisory mission shall be carried out in compliance with the applicable national law of the Member State where that infrastructure is located.

8. When organising the advisory missions, the Commission shall take into account the reports of any inspections carried out by the Commission under Regulation (EC)

300/2008 and Regulation (EC) 725/2004 and of the reports of any monitoring carried out by the Commission under Directive 2005/65/EC in respect of the critical entity or the critical entity of particular European significance, as appropriate.

CHAPTER V
COOPERATION AND REPORTING

Article 16
Critical Entities Resilience Group

1. A Critical Entities Resilience Group is established with effect from [six months after the entry into force of this Directive]. It shall support the Commission and facilitate strategic cooperation 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. Where relevant for the performance of its tasks, the Critical Entities Resilience Group may invite representatives of interested parties to participate in its work.

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

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

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

   (b) evaluating the strategies on the resilience of critical entities referred to in Article 3 and identifying best practices in respect of those strategies;

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

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

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

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

   (g) analyse and provide advice on the reports of advisory missions in accordance with Article 15(3);

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

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

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

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

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

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

Article 17
Commission support to competent authorities and critical entities

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

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

CHAPTER VI
SUPERVISION AND ENFORCEMENT

Article 18
Implementation and enforcement

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

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

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

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

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

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

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

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

4. Member State shall ensure that the powers provided for in paragraphs 1, 2 and 3 can only be exercised subject to appropriate safeguards. Those safeguards shall guarantee, in particular, that such exercise takes place in an objective, transparent and proportionate manner and that the rights and legitimate interests of the critical entities affected are duly safeguarded, including their rights to be heard, of defence and to an effective remedy before an independent court.

5. Member States shall ensure that, when a competent authority assesses the compliance of a critical entity pursuant to this Article, it shall inform the competent authorities of the Member State concerned designated under the [the NIS 2 Directive] and may request those authorities to assess the cybersecurity of such entity, and cooperate and exchange information for this purpose.

Article 19
Penalties

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

CHAPTER VII
FINAL PROVISIONS

Article 20
Committee procedure

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

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

Article 21
Exercise of the delegation

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

2. The power to adopt delegated acts referred to in Article 11(4) shall be conferred on the Commission for a period of five years from date of entry into force of this Directive or any other date set by the co-legislators.

3. The delegation of power referred to in Article 11(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

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

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

6. A delegated act adopted pursuant to Article 11(4) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 22
Reporting and review

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

The Commission shall periodically review the functioning of this Directive, and report to the European Parliament and to the Council. The report shall in particular assess the impact and added value of this Directive on ensuring the resilience of critical entities and whether the scope of the Directive should be extended to cover other sectors or subsectors. The first report shall be submitted by [six years after the entry into force of this Directive] and shall assess in particular whether the scope of the Directive should be extended to include the food production, processing and distribution sector.

Article 23
Repeal of Directive 2008/114/EC

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

Article 24
Transposition

1. Member States shall adopt and publish, by [18 months after entry into force of this Directive] at the latest, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith communicate to the Commission the text of those provisions.

   They shall apply those provisions from [two years after entry into force of this Directive + one day].

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

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

Article 25
Entry into force

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

Article 26
Addressees

This Directive is addressed to the Member States.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the resilience of critical entities

1.2. Policy area(s) concerned

Security

1.3. The proposal/initiative relates to:

☐ **a new action**

☐ **a new action following a pilot project/preparatory action**[40]

☑ **the extension of an existing action**

☐ **a merger or redirection of one or more actions towards another/a new action**

1.4. Objective(s)

1.4.1. General objective(s)

The operators of critical infrastructures provide services in a number of sectors (such as transport, energy, health, water, etc.) which are necessary for vital societal functions and economic activites. The operators therefore need to be resilient, i.e. well protected, but also able to rapidly come back into operations in the event of disruption.

The general objective of the proposal is to enhance the resilience of these operators (referred here as 'critical entities') against a range of natural and man-made, intentional or unintentional risks.

1.4.2. Specific objective(s)

The intiative aims to adress four specific objectives:

- to ensure a higher of level of understanding of risks and interdependencies faced by critical entities, as well as the means to address them;

- to ensure that all relevant entities are designated as 'critical entities' by Member States authorities;

- to ensure that the full spectrum of resilience activities is included in public policies and operational practice;

- to strengthen capacities and improve cooperation and communication between stakeholders.

These objectives will contribute to achieving the general objective of the intitiave.

1.4.3. Expected result(s) and impact

Specify the effects which the proposal/initiative should have on the beneficiaries/groups targeted.

[40] As referred to in Article 58(2)(a) or (b) of the Financial Regulation.

The initiative is expected to have positive effects on the security of critical entities, which would be more resilient to risks and disruptions. They would be able to better mitigate risks, deal with potential disruptions, and minimise negative impacts in cases where incident occur.

Better resilience of critical entities also means that their operations will be more reliable and their services across many vital sectors provided in a continious fashion, contributing to a smooth functioning of the internal market. This will in turn have positive impact for the general public and businesses, as they rely in their daily activities on these services.

Public authorities would also benefit from the stability derived from the smooth functioning of key economic activities and the constant provision of essential services to their citizens.

1.4.4. Indicators of performance

Specify the indicators for monitoring progress and achievements.

Indicators for monitoring progress and achievements will be linked to the specific objectives of the initative:

- the number and scope of risk assessments by authorities and critical entities will be a proxy of the higher understanding of risks by key actors.

- the number of 'critical entities' identified by Member States will be a reflection of the comprehensiveness of critical infrastructure policies coverage.

- the mainstreaming of resilience in public policies and operational practice will be reflected in the national strategies and critical entities' resilience measures.

- improvements in terms of capacities and cooperation will be assessed on the basis of capacity building activities and cooperation initiatives developed.

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative

To meet the requirements of the inititative, the Member States will need to, in the short to medium term, develop a strategy on the resilience of critical entities; conduct national risk assessment; and identify which operators are 'critical entities' on the basis of the outcomes of the risk assessment and specific criteria. These activities will be carried out regularly as necessary, and at least once every four years. The Member States will also have to establish mechanisms for cooperation between relevant stakeholders.

The operators designated as 'critical entities' would be required to, in the short to medium term, carry out risk assessment of their own; take appropriate and proportionate technical and organisational measures to ensure their resilience; and notify competent authorities of incidents.

1.5.2. Added value of Union involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this point 'added value of Union involvement' is the value resulting from Union intervention which is additional to the value that would have been otherwise created by Member States alone.

Reasons for action at European level (ex-ante): The objective of this initiative is to enhance the resilience of critical entities against a range of risks. This objective cannot be sufficiently achieved by the Member States acting alone: the EU action is justified due to the common nature of risks that critical entities face; the transnational character of the services they provide; and the interdependencies and connections between them (across the sectors and borders). This means that a vulnerability or a disruption of one single facility has the potential to create disruption across sectors and borders. Expected generated Union added value (ex-post): Compared to current situation, the proposed initiative will add value in particular by: - establishing a general framework that would promote closer alignment of Member States policies (consistent sectoral scope, criteria to designate critical entities, common requirements in terms of risk assessments), - ensuring that critical entities take appropriate resilience measures, - bringing together knowledge and expertise from across the EU that would optimise the response of critical entities and authorities, - reducing the discrepancies between Member States and leveling up the resilience of critical entities across the EU.

1.5.3. Lessons learned from similar experiences in the past

The proposal draws on the lessons learnt from the implementation of the Directive on on European Critical Infrastructures (Directive 2008/114/EC) and its evaluation (SWD(2019) 308).

1.5.4. Compatibility with the Multiannual Financial Framework and possible synergies with other appropriate instruments

This proposal is one of the building blocks of the new EU Security Union Strategy aimed at achieving a future-proof security environment. Synergies can be developed with the Union Civil Protection Mechanism in relation to disaster prevention, mitigation and management.

1.6. Duration and financial impact of the proposal/initiative

☐ **limited duration**

☐ in effect from [DD/MM]YYYY to [DD/MM]YYYY

☐ Financial impact from YYYY to YYYY for commitment appropriations and from YYYY to YYYY for payment appropriations.

☑ **unlimited duration**

- Implementation with a start-up period from 2021 to 2027,
- followed by full-scale operation.

1.7. Management mode(s) planned[41]

☑ **Direct management** by the Commission

☑ by its departments, including by its staff in the Union delegations;

☐ by the executive agencies

☑ **Shared management** with the Member States

☐ **Indirect management** by entrusting budget implementation tasks to:

☐ third countries or the bodies they have designated;

☐ international organisations and their agencies (to be specified);

☐ the EIB and the European Investment Fund;

☐ bodies referred to in Articles 70 and 71 of the Financial Regulation;

☐ public law bodies;

☐ bodies governed by private law with a public service mission to the extent that they provide adequate financial guarantees;

☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that provide adequate financial guarantees;

☐ persons entrusted with the implementation of specific actions in the CFSP pursuant to Title V of the TEU, and identified in the relevant basic act.

If more than one management mode is indicated, please provide details in the 'Comments' section.

Comments

Direct management will cover primarily: administrative expenses for DG HOME, Administrative Arrangement with JRC, grants managed by Commission. Shared management will cover: Projects under shared management: Member States will need to develop a strategy and risk assessment, and may use their national envelopes for these purposes.

[41] Details of management modes and references to the Financial Regulation may be found on the BudgWeb site: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

Specify frequency and conditions.

As per the proposal for a Regulation of the European Parliament and of the Council establishing, as part of the Internal Security Fund, the Union's instrument dedicated to the area of security (COM(2018) 472 final):

Shared management:

Each Member State shall establish a management and control systems for its programme and ensure the quality and the reliability of the monitoring system and of data on indicators, in accordance with the Common Provision Regulation (CPR). In order to facilitate a swift start of implementation, it is possible to 'roll-over' existing well-functioning management and control systems to the next programming period.

In this context, Member States will be requested to set up a monitoring committee to which the Commission shall participate in an advisory capacity. The monitoring committee shall meet at least once a year. It shall review all issues that affect programme progress towards achieving its objectives.

The Member States will send an annual performance report, which should set out information on the progress in the implementation of the programme and in achieving the milestones and targets. It should also raise any issues affecting the performance of the programme and describe the action taken to address them.

At the end of the period, each Member States shall submit a final performance report. The final report should focus on the progress made towards achieving the objectives of the programme and should give an overview of the key issues that affected the programme's performance, the measures taken to address those issues and the assessment of the effectiveness of these measures. In addition it should present the contribution of the programme to tackling the challenges identified in the relevant EU recommendations addressed to the Member State, the progress made in achieving the targets set out in the performance framework, the findings of the relevant evaluations and the follow-up given to those findings and the results of the communication actions.

According to the draft CPR proposal, the Member States shall send each year an assurance package, which includes the annual accounts, the management declaration and the audit authority's opinions on the accounts, the annual control report as required by Article 92(1)(d) of CPR, the management and control system and the legality and regularity of the expenditure declared in the annual accounts. This assurance package will be used by the Commission to determine the amount chargeable to the Fund for the accounting year.

A review meeting between the Commission and each Member State shall be organised every two years to examine the performance of each programmes.

The Member States send 6 times per year data for each programme broken down by specific objectives. These data refers to the cost of operations and the values of common output and result indicators.

In general:

The Commission shall carry out a mid-term and a retrospective evaluation of the actions implemented under this Fund, in line with the Common Provisions Regulation. The mid-term evaluation should be based in particular on the mid-term evaluation of programmes submitted to the Commission by the Member States by 31 December 2024.

2.2. Management and control system(s)

2.2.1. Justification of the management mode(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

As per the proposal for a Regulation of the European Parliament and of the Council establishing, as part of the Internal Security Fund, the Union's instrument dedicated to the area of security (COM(2018) 472 final):

Both the ex-post evaluations of the DG HOME 2007-2013 Funds and the interim evaluations of the current DG HOME Funds show that a mix of delivery modes in the areas of migration and home affairs allowed for an effective way to achieve the objectives of the Funds. The holistic design of the delivery mechanisms is maintained and includes shared, direct and indirect management.

Through shared management Member States implement programmes that contribute to the policy objectives of the Union, which are tailor-made to their national context. Shared management ensures that financial support is available in all participating States. Furthermore, shared management allows for funding predictability and for Member States, who are most knowledgeable of the challenges they are faced with, to plan their long-term endowments accordingly. As a novelty, the Fund can also provide emergency assistance through shared management, in addition to direct and indirect management.

Through direct management, the Commission supports other actions that contribute to the common policy objectives of the Union. The actions enable tailor made support for urgent and specific needs in individual Member States ("emergency assistance"), support transnational networks and activities, test innovative activities that could be scaled up under national programmes and cover studies in the interest of the Union as a whole ("Union actions").

Through indirect management, the Fund retains the possibility to delegate budget implementation tasks to, among others, International Organisations and Home Affairs Agencies for particular purposes.

Bearing in mind the different objectives and needs, a thematic facility is proposed under the Fund as a way to balance the predictability of multiannual allocation of funding to the national programmes with flexibility in disbursing funding periodically to actions with a high level of added value to the Union. The thematic facility will be used for specific actions in and amongst Member States, Union actions, emergency assistance. It will ensure that funds can be allocate and transferred among the different modalities above, on the basis of a two yearly programming.

The payment modalities for shared management are described in the draft CPR proposal, which foresees an annual pre-financing, followed by a maximum of 4 interim payments per programme and year based on the payment applications sent by the Member States during the accounting year. As per the draft CPR proposal the pre-financing are cleared within the final accounting year of the programmes.

The control strategy will be based on the new Financial Regulation and on the Common Provision Regulation. The new Financial Regulation and the draft proposal for CPR should extend the use of the simplified forms of grants such as lump-sums, flat rates and unit costs. It also introduces new forms of payments, based on the results achieved, instead of the cost. Beneficiaries will be able to receive a fixed amount of money if they prove that certain actions such as trainings or delivery of humanitarian assistance have taken place. This is expected to simplify the control burden both at beneficiary and Member State level (e.g. check of bills and receipts for costs).

For shared management, the draft CPR proposal builds on the management and control strategy in place for the 2014-2020 programming period but introduces some measures aimed at simplifying the implementation and reducing the control burden at the level of both beneficiaries and Member States. The novelties include:

- the removal of the designation procedure (which should allow to speed up the implementation of the programmes)

- management verifications (administrative and on-the-spot) to be carried out by the managing authority on a risk-basis (compared to the 100% administrative controls required in the 2014-2020 programming period). Furthermore, under certain conditions, the managing authorities may apply proportionate control arrangements in line with the national procedures.

- conditions to avoid multiple audits on the same operation/expenditure

The programme authorities will submit to the Commission interim payment claims based on expenditure incurred by beneficiaries. The draft CPR proposal allows the managing authorities to carry out management verifications on a risk-basis and foresees also specific controls (e.g. on-the-spot controls by the managing authority and audits of operations/expenditure by the audit authority) after the associated expenditure has been declared to the Commission in the interim payment claims. In order to mitigate the risk of reimbursing ineligible expenditure, the draft CPR foresees the Commission's interim payments to be capped at 90%, given that at this moment only part of the national controls have been carried out. The Commission will pay the remaining balance following the annual clearance of accounts exercise, upon receipt of the assurance package from the programme authoirties. Any irregularities detected by the Commisson or the European Court of Auditors after the transmission of the annual assurance package may lead to a net financial correction.

For the part implemented through **direct management** under the thematic facility, the management and control system will build on the experience gained in 2014-2020 in both Union actions and emergency assistance. A simplified scheme will be established allowing a swift processing of the applications for funding while reducing the risk of errors: eligible applicants will be limited to Member States and International organisations, funding will be based on simplified cost options, standard templates will be developed for funding applications, grant/contribution agreements and reporting, a standing evaluation committee will examine the applications as soon as they are received.

2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

DG HOME has not been facing important risks of errors in its spending programmes. This is confirmed by the recurrent absence of significant findings in the annual reports of the Court of Auditors.

In shared management, the general risks in relation to the implementation of the current programmes concerns the under-implementation of the Fund by the Member States and the possible errors derived from the complexity of rules and weaknesses in management and control systems. The draft CPR simplifies the regulatory framework by harmonising the rules and management and control systems across the different Funds implemented under shared management. It simplifies also the control requirements (e.g. risk-based management verifications, possibility for proportionate control arrangements based on national procedures, limitations of audit work in terms of timing and/or specific operations).

2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio of "control costs ÷ value of the related funds managed"), and assessment of the expected levels of risk of error (at payment & at closure)

The ratio of "control costs/value of the related funds mananged)" is reported on by the Commission. The 2019 AAR of DG HOME reports 0.72% for this ratio in relation to shared management, 1.31% for direct management grants and 6.05% for direct management procurement. For shared management, this percentage usually decreases over time with efficiency gains in implementation of the programmes and increase in payments to Member States.

With the risk based approach to management and controls being introduced in the draft CPR coupled with enhanced drive to adopt simplified cost options (SCOs), the cost of controls for Member States is expected to be reduced further.

The Annual Activity Report 2019 reported a cumulative residual error rate of 1.57% for AMIF/ISF National Programmes and a cumulative residual error rate of 4.11% for non-research direct management grants.

2.3. Measures to prevent fraud and irregularities

Specify existing or envisaged prevention and protection measures, e.g. from the Anti-Fraud Strategy.

DG HOME will continue to apply its Anti-Fraud Strategy in line with the Commission's Anti-Fraud Strategy (CAFS) in order to ensure inter alia that its internal anti-fraud related controls are fully aligned with the CAFS and that its fraud risk management approach is geared to identify fraud risk areas and adequate responses.

As regards shared management, Member States shall ensure the legality and regularity of expenditure included in the account submitted to the Commission. In this context, Member States shall take all required actions to prevent, detect and correct irregularities. As in the present programming cycle 2014-2020 Member States are obliged to put in place procedures for detection of irregularities and anti-fraud coupled with the specific Commission Delegated Regulation on reporting of irregularities. Anti-Fraud measures will remain a cross-cutting principle and obligation for Member States.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

(1) New budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Heading No. 5: Resilience, Security and Defence	Diff./Non-diff.[42]	from EFTA countries [43]	from candidate countries[44]	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation
5	12.02.01 – "Internal Security Fund"	Diff.	NO	NO	YES	NO
5	12 01 01 - Support expenditure for the "Internal Security Fund"	Non-diff.	NO	NO	YES	NO

Comment:

It should be noted that operational appropriations requested in the context of the proposal are covered by appropriations already foreseen in the LFS underlying the ISF Regulation.

Additional human resources are requested in the context of this legislative proposal.

[42] Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.

[43] EFTA: European Free Trade Association.

[44] Candidate countries and, where applicable, potential candidates from the Western Balkans.

3.2. Estimated financial impact of the proposal on appropriations

3.2.1. Summary of estimated impact on operational appropriations

☐ The proposal/initiative does not require the use of operational appropriations

☑The proposal/initiative requires the use of operational appropriations, as explained below:

EUR million (to three decimal places)

Heading of multiannual financial framework	5	Resilience, Security and Defence

DG: HOME			2021	2022	2023	2024	2025	2026	2027	**Post-2027**	**TOTAL**
• Operational appropriations											
Budget line 12 02 01 Internal Security Fund	Commitments	(1a)	0,124	4,348	5,570	6,720	7,020	7,020	7,020		37,822
	Payments	(2a)	0,540	4,323	5,357	5,403	5,403	5,403	5,403	5,989	37,822
Appropriations of an administrative nature financed from the envelope of specific programmes[45]											
Budget line		(3)									
TOTAL appropriations for DG HOME	Commitments	=1a+1b +3	0,124	4,348	5,570	6,720	7,020	7,020	7,020		37,822
	Payments	=2a+2b +3	0,540	4,323	5,357	5,403	5,403	5,403	5,403	5,989	37,822

[45] Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

• TOTAL operational appropriations	Commitments	(4)									
	Payments	(5)									
• TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)									
TOTAL appropriations under HEADING 5 of the multiannual financial framework	Commitments	=4+ 6	0,124	4,348	5,570	6,720	7,020	7,020	7,020		37,822
	Payments	=5+ 6	0,540	4,323	5,357	5,403	5,403	5,403	5,403	5,989	37,822

If more than one operational heading is affected by the proposal / initiative, repeat the section above:

• TOTAL operational appropriations (all operational headings)	Commitments	(4)									
	Payments	(5)									
TOTAL appropriations of an administrative nature financed from the envelope for specific programmes (all operational headings)		(6)									
TOTAL appropriations under HEADINGS 1 to 6 of the multiannual financial framework (Reference amount)	Commitments	=4+ 6	0,124	4,348	5,570	6,720	7,020	7,020	7,020		37,822
	Payments	=5+ 6	0,540	4,323	5,357	5,403	5,403	5,403	5,403	5,989	37,822

Heading of multiannual financial framework	7	'Administrative expenditure'

This section should be filled in using the 'budget data of an administrative nature' to be firstly introduced in the Annex to the Legislative Financial Statement (Annex V to the internal rules), which is uploaded to DECIDE for interservice consultation purposes.

EUR million (to three decimal places)

		2021	2022	2023	2024	2025	2026	2027	**TOTAL**
DG: HOME									
• Human resources		0,152	0,228	0,499	0,813	0,932	0,932	0,932	**4,488**
• Other administrative expenditure		0,033	0,085	0,109	0,109	0,109	0,109	0,109	**0,663**
TOTAL DG HOME	Appropriations	**0,185**	**0,313**	**0,608**	**0,922**	**1,041**	**1,041**	**1,041**	**5,151**

TOTAL appropriations under HEADING 7 of the multiannual financial framework	(Total commitments = Total payments)	**0,185**	**0,313**	**0,608**	**0,922**	**1,041**	**1,041**	**1,041**	**5,151**

EUR million (to three decimal places)

		2021	2022	2023	2024	2025	2026	2027	**Post 2027**	**TOTAL**
TOTAL appropriations under HEADINGS 1 to 7 of the multiannual financial framework	Commitments	**0,309**	**4,661**	**6,178**	**7,642**	**8,061**	**8,061**	**8,061**	**-**	**42,973**
	Payments	**0,725**	**4,636**	**5,965**	**6,325**	**6,444**	**6,444**	**6,444**	**5,989**	**42,973**

3.2.2. *Estimated output funded with operational appropriations*

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs			Year **2021**		Year **2022**		Year **2023**		Year **2024**		Year **2025**		Year **2026**		Year **2027**		TOTAL	
⇩	Type	Average cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost
SPECIFIC OBJECTIVE NO 1: Commission support to competent authorities and critical entities																		
Output	Developing and maintaining the knowledge and support capacity					2.000		2.000		2.000		2.000		2.000		2.000		12.000
Output	Support to competent authorities by fostering the exchange of best practices and information and by carrying out risk assessments (The financial costs covered by studies below)					-												
Output	Support to competent authorities and critical entities (i.e. operators) by developing guidance materials and methodologies, supporting the organisation of exercises simulating real-time incident scenarios, providing training					0.500		0.850		1.200		1.500		1.500		1.500		7.050
Output	Projects on various topics related to support activities mentioned above (risk assessment methodologies, simulations of real-time incident scenarios, trainings…)	0.400			3	1.200	5	2.000	7	2.800	7	2.800	7	2.800	7	2.800	36	14.400
Output	Studies (risk assessments) and consultations (related to implementation of the Directive)	0.100			4	0.400	4	0.400	4	0.400	4	0.400	4	0.400	4	0.400	24	2.400
Output	Other meetings, conference	0.031	4	0.124	8	0.248	8	0.248	8	0.248	8	0.248	8	0.248	8	0.248	52	1.612
Subtotal for specific objective N°1				0.124		4.348		5.498		6.648		6.948		6.948		6.948		37.462
SPECIFIC OBJECTIVE NO 2: Resilience Advisory teams																		
- Output	Organisation of Resilience advisory teams (Members: Member States representatives). COM to organise call for members (for MS participants)																	-
- Output	COM to organise the programme and advisory missions COM to provide substantial input to advisory missions (guidance and oversight of Critical entities of European significance – together with MS) Day-to-day coordination of Resilience advisory teams							0.072		0.072		0.072		0.072		0.072		0.360
Subtotal for specific objective N°2								0.072		0.072		0.072		0.072		0.072		0.360
TOTAL for objectives 1 to 2				**0.124**		**4.348**		**5.570**		**6.720**		**7.020**		**7.020**		**7.020**		**37.822**

3.2.3. Summary of estimated impact on administrative appropriations

☐ The proposal/initiative does not require the use of appropriations of an administrative nature

☑ The proposal/initiative requires the use of appropriations of an administrative nature, as explained below:

EUR million (to three decimal places)

	2021	2022	2023	2024	2025	2026	2027	TOTAL
HEADING 7 of the multiannual financial framework								
Human resources	0,152	0,228	0,499	0,813	0,932	0,932	0,932	4,488
Other administrative expenditure	0,033	0,085	0,109	0,109	0,109	0,109	0,109	0,663
Subtotal HEADING 7 of the multiannual financial framework	**0,185**	**0,313**	**0,608**	**0,922**	**1,041**	**1,041**	**1,041**	**5,188**

Outside HEADING 7[46] of the multiannual financial framework								
Human resources								
Other expenditure of an administrative nature								
Subtotal outside HEADING 7 of the multiannual financial framework								

TOTAL	**0,185**	**0,313**	**0,608**	**0,922**	**1,041**	**1,041**	**1,041**	**5,188**

The appropriations required for human resources and other expenditure of an administrative nature will be met by appropriations from the DG that are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

[46] Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

3.2.3.1. Estimated requirements of human resources

☐ The proposal/initiative does not require the use of human resources.

☑ The proposal/initiative requires the use of human resources, as explained below:

Estimate to be expressed in full time equivalent units

		Year **2021**	Year **2022**	Year **2023**	Year **2024**	2025	2026	2027
• Establishment plan posts (officials and temporary staff)								
20 01 02 01 (Headquarters and Commission's Representation Offices)		1	2	4	5	5	5	5
XX 01 01 02 (Delegations)								
XX 01 05 01/11/21 (Indirect research)								
10 01 05 01/11 (Direct research)								
• External staff (in Full Time Equivalent unit: FTE)[47]								
20 02 01 03 (AC, END, INT from the 'global envelope')				1	2	2	2	2
XX 01 02 02 (AC, AL, END, INT and JPD in the delegations)								
XX 01 04 **yy** [48]	- at Headquarters							
	- in Delegations							
XX 01 05 02/12/22 (AC, END, INT - Indirect research)								
10 01 05 02/12 (AC, END, INT - Direct research)								
Other budget lines (specify)								
TOTAL		**1**	**2**	**5**	**7**	**7**	**7**	**7**

XX is the policy area or budget title concerned.

The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

Description of tasks to be carried out:

Officials and temporary staff	The proposal assumes 4 AD and 1 AST dedicated to the implementation of the Directive on the side of the Commission, of which 1 AD is already in-house and the remaining FTE constitute additional human resources to be recruited. The recruitment plan foresees: 2022: +1 AD: policy officer responsible for setting up the knowledge capacity and support activities 2023: +1 AD (policy officer responsible for the Advisory teams), 1 AST (Assistant for Resilience Advisory teams) 2024: +1 AD (policy officer contributing to support activities to authorities and operators)
External staff	The proposal assumes 2 SNEs dedicated to the implementation of the Directive on the side of the Commission. The recruitment plan foresees: 2023: +1 END (Critical Infrastructure resilience expert / contributing to support activities to authorities and operators)

[47] AC= Contract Staff; AL = Local Staff; END= Seconded National Expert; INT = agency staff; JPD= Junior Professionals in Delegations.

[48] Sub-ceiling for external staff covered by operational appropriations (former 'BA' lines).

	2024: + 1 END (Critical Infrastructure resilience expert / contributing to support activities to authorities and operators)

3.2.4. Compatibility with the current multiannual financial framework

The proposal/initiative:

☑ can be fully financed through redeployment within the relevant heading of the Multiannual Financial Framework (MFF).

Operational expenditure covered by ISF under MFF 2021-2027

☐ requires use of the unallocated margin under the relevant heading of the MFF and/or use of the special instruments as defined in the MFF Regulation.

Explain what is required, specifying the headings and budget lines concerned, the corresponding amounts, and the instruments proposed to be used.

☐ requires a revision of the MFF.

Explain what is required, specifying the headings and budget lines concerned and the corresponding amounts.

3.2.5. Third-party contributions

The proposal/initiative:

☑ does not provide for co-financing by third parties

☐ provides for the co-financing by third parties estimated below:

Appropriations in EUR million (to three decimal places)

	Year **N**[49]	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)			Total
Specify the co-financing body								
TOTAL appropriations co-financed								

[49] Year N is the year in which implementation of the proposal/initiative starts. Please replace "N" by the expected first year of implementation (for instance: 2021). The same for the following years.

3.3. Estimated impact on revenue

☑ The proposal/initiative has no financial impact on revenue.

☐ The proposal/initiative has the following financial impact:

☐ on own resources

☐ on other revenue

please indicate, if the revenue is assigned to expenditure lines ☐

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative[50]						
		Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)		
Article …….								

For assigned revenue, specify the budget expenditure line(s) affected.

[…]

Other remarks (e.g. method/formula used for calculating the impact on revenue or any other information).

[…]

[50] As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 20 % for collection costs.