POSITION PAPER

RESILIENCE OF CRITICAL ENTITIES

This position paper constitutes FEDIL's contribution to the Proposal for a directive of the European Parliament and of the Council on measures for high common level of cybersecurity across the Union, repealing directive (EU) 2016/1148 ("NIS 2 directive") and to the Proposal for a directive of the European Parliament and of the Council on the resilience of critical entities ("CER directive").

CONTEXT

The digitization of our industry, our economy and our society has brought about important challenges in terms of cybersecurity and resilience. New forms of cyberattacks constantly emerge and the acceleration of the digital transition and interconnectedness emphasized by the COVID-19 crisis has made cybercrimes a daily reality.

According to the European Commission's science and knowledge service, the Joint Research Centre, in 2020, the annual cost of cybercrimes to the global economy is estimated to be €5.5 trillion. The most frequent targets of cyberattacks are digital services, the finance sector but also the manufacturing and public sectors. In 2019, around 450 cybersecurity incidents involved European critical infrastructures such as finance or energy[1].

The pace and complexity of cyberattacks are growing and the capabilities of attackers from all over the world to threaten our security and our freedoms should not be underestimated. Robust and innovative responses are essential to build trust in our digital infrastructures.

In this context, the European Union puts cybersecurity as a priority response to the COVID-19 crisis. On 16 December 2020, the European Commission presented a new cybersecurity package, which builds upon existing instruments and presents new initiatives to further improve EU cyber resilience and response. The objective of the new EU Cybersecurity Strategy published with this package is to make sure that citizens and businesses benefit from trustworthy and reliable services as well as digital tools. To reinforce Europe's collective resilience against cyber threats, to improve the resilience and incident response capacities of public and private entities, competent authorities, and the European Union in the field of cybersecurity and critical infrastructure protection, the strategy is accompanied by two new proposals – the NIS 2 directive for a high common level of cybersecurity across the Union (I.) and the CER directive on the resilience of critical entities (II.).

Although the CER directive addresses physical resilience and the NIS 2 directive focuses on cyber resilience, both proposals will impact critical entities and information networks. To avoid a disconnection between various prerequisites and potential conflicts between requirements in both texts, it is essential to align the proposed directives as much as possible.

[1] https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f

POSITION PAPER

RESILIENCE OF CRITICAL ENTITIES

TABLE OF CONTENT

POSITION PAPER

RESILIENCE OF CRITICAL ENTITIES

I. NIS 2.0 DIRECTIVE

As cyber resilience and incident response capacities must always be adapted and reinforced, FEDIL welcomes the European Commission's proposal for a NIS 2 directive which will improve critical infrastructures' protection.

We strongly support the proposed directive's objective to further harmonize enforcement measures and sanction regimes as well as security and reporting requirements in order to facilitate regulatory compliance for entities providing cross-border services.

Luxembourg's industry believes the proposed NIS 2 directive is key to improving the EU's ability to prepare and respond to cyberattacks collectively and thus strengthening its overall resilience by creating a common ground. Indeed, cooperation between Member States must be expanded, especially as regards information sharing and crisis management. The margin left to Member States for the implementation of the first NIS directive led to inconsistencies in the internal market, notably concerning the identification of the companies to be in the scope of the current rules. Consequently, comparable companies of similar size are included within the scope in one Member State but not in another. In this context, FEDIL supports a risk-based approach and welcomes the classification of entities based on their importance and divided respectively in essential and important entities with the consequence of being subjected to different supervisory regimes. Indeed, the classification should be based on the risk their activities entail and the importance of those on the local and global economy and stability.

Our members also agree with the inclusion of new sectors into the general remit of the NIS 2 directive to focus on their criticality for the economy and the society. For instance, in Annex I, point 8.; "*Providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972 (EECC) or* ***providers of electronic communications services*** *referred to in point (4) of Article 2 of Directive (EU) 2018/1972 (EECC) where their services are publicly available*" are proposed to be covered by the NIS 2.0 directive as essential entities. We understand that such entities will have to comply with cybersecurity requirements set in the proposed directive instead of those today included in the European Electronic Communications Code. Our members support this provision since it is more efficient to have one common framework covering several sectors for essential and important services rather than a fragmented one. However, some sectors deserve further clarification as regards their definition and scope. The space sector for example, is identified as "*Operators of ground-based infrastructure, owned, managed and operated* ***by Member States or by private parties****, that support the provision of space-based services, excluding providers of public electronic communications networks*". By targeting any infrastructure supporting space-based services, all services provided from space might potentially fall within the scope of the NIS 2 directive, including services that are not for the telecommunications. This would also lead to a difference of treatment with terrestrial telecommunications infrastructure provider regarding public and private network and services. While the "digital Infrastructure sector" (covering both satellite and terrestrial operations) identify only providers of electronic communications networks that are public, or providers of electronic communications services where their services are publicly available, that potentially all space-based services are covered whether they are public or not. We do not believe this would be consistent with the purpose of the directive which aims to enhance the resilience of critical entities providing essential services to the society.

RESILIENCE OF CRITICAL ENTITIES

We also support the idea of a size cap according to which only medium and large companies will be included in the scope while still maintaining a certain flexibility for Member States to include small and micro entities with a high-security risk profile. We are convinced this will balance out the burdens put on companies and public administrations.

Additionally, we appreciate that the future NIS 2 directive requires selected providers of digital infrastructure or digital services which do not have a European establishment but offer services in the EU to respect the same rules. Still, this improved "level playing field" remains to be confirmed by the ability of national authorities to enforce the new measures.

POSITION PAPER

RESILIENCE OF CRITICAL ENTITIES

A) COOPERATION

Our members generally welcome the proposed provisions to improve cooperation and information exchange within the EU. More specifically, on the frameworks for **coordinated vulnerability disclosure** laid down in article 6, we support the designation of one of the CSIRTs to act as trusted intermediary and facilitate the interaction between the reporting entities and the manufacturers and providers of ICT products or services. However, we also encourage Coordinated Vulnerability Disclosure policies that leverage the existing Common Vulnerability and Exposure registry and believe vulnerability researchers should have the possibility to report vulnerabilities directly to the manufacturers and use intermediaries optionally. The opportunity to directly contact manufacturers and providers of ICT products or services to address any vulnerability should also be given to researchers without obliging them to disclose the research.

Moreover, we believe manufacturers and providers of ICT products or services should have the possibility to address their vulnerability issues internally and remedy possible problems before they are made public. Indeed, once vulnerabilities are made public in the European vulnerability registry for the discovered vulnerabilities, to be developed by ENISA, companies become an easier target to cyberattacks.

B) RISK MANAGEMENT & REPORTING

1. GOVERNANCE

The proposed article 17 of the NIS 2 directive intends to submit the management body of subjected entities to new governance requirements. According to the proposal, the management body would have to approve and supervise the cybersecurity risk management measures laid down in the proposed article 18 and follow specific cybersecurity trainings. Furthermore, the management body would be held accountable for the non-compliance with cybersecurity risk management measures of the entity concerned.

Governance requirements for management bodies will contribute to making cybersecurity being treated as an important topic by subjected entities. However, what is included in the definition of a "management body" under the proposed directive should be clarified as it can vary significantly depending on the size and structure of a company.

As regards cybersecurity trainings, FEDIL believes more attention should be given to cybersecurity trainings which target people without an IT background, knowledge or work practice and regular users of digital technologies. Cybersecurity should not only be the responsibility of the CISO and training needs to be provided at all levels as security and resilience is the responsibility of any single individual entering a company, physically or virtually.

Although, it is true that management bodies of companies do not always have the most relevant or sufficient knowledge on cybersecurity. Indeed, the organization's management should be trained to acquire essential and basic cybersecurity knowledge and skills, in order to be able to address the specific cybersecurity needs of the concerned entity. Still, more clarification on the type of training is needed as most trainings are nowadays targeted at experienced IT experts.

While each board member should have the topic on the radar and be equally accountable for non-compliance with cybersecurity risk management measures, we would recommend appointing one board member to oversee the organization's cybersecurity risk management and to be a key enabler to drive cybersecurity needs of the concerned entity.

2. RISK MANAGEMENT MEASURES

We welcome the proposed risk management measures in article 18 insofar that entities will be required to take only those **measures necessary and proportionate to the risk** posed by their security of network and information system. This will allow organizations to address the most recent cybersecurity risks and remains very important to minimize compliance costs for SMEs and reduce unnecessary regulatory burdens on them.

Article 18 also proposes a risk management-based approach in providing the **minimum requirements of baseline security elements** that must be adopted and applied. Considering that those requirements will have to be established by the Member States during the transposition of the directive, we observe an important risk of fragmentation. Indeed, if some Member States expand the minimum requirements of baseline security further at national level, entities might have to comply with 27 different baseline security elements according to the location of their activities. This would harm the functioning of the internal market and cross-border provision of essential services. The NIS 2 directive should apply the country-of-origin principle, recognizing a company's compliance in the Member State of destination of its services if it is compliant with the security requirements in the country where its main establishment is located.

The proposal under article 18 §1 (d) and article 18 §3 requires individual companies to address **cybersecurity risks in supply chains and supplier relationships.** Entities may need to ensure that their contracts with third-party suppliers include a minimum set of cybersecurity requirements such as, for instance:

- The third-party supplier informs the entity about any potential cybersecurity event or activity discovered or detected. It could be required to inform the entity no later than 24 hours after detection to minimize the potential impact.
- In case of outsourcing of the IT infrastructure or business application, the entity ensures that the outsourcing organization has the same level of security and compliance and provides SAE16 or ISAE3402 reports on a yearly basis, confirming an appropriate level of security.
- In case of outsourcing of the IT infrastructure or business application, the entity remains responsible for the level of security and compliance of the outsourcing organization. The entity is doing compliance controls implemented by the outsourcing organization and is responsible for independent audit activities to confirm an appropriate level of security.

However, FEDIL would like to express its concerns regarding new requirements to manage third-party cybersecurity risks in supply chains and supplier relationships. To implement supply chain security, this concept must first be clearly defined at European level under the new NIS 2 directive. Depending on the definition of supply chain, it will be challenging for businesses that operate in large global supply chains to take account of vulnerabilities specific to each supplier and each services provider.

Regarding the security measures to be taken, each entity under the NIS 2 directive will have to monitor its own threat landscape, regarding its own activities and customers too. This confirms our urgent call for measures and policies to **increase the number of cybersecurity experts**. In 2021, it appears still challenging for companies to find and hire cybersecurity experts.

3. REPORTING OBLIGATIONS

Article 20 of the proposed NIS 2 directive introduces a very precise process for **incident reporting,** harmonizing the content of the reports and the timelines. This article is expanding reporting obligations, in terms of what must be reported, to whom the reports must be sent, and within what timeframe.

For instance, the proposal foresees an initial notification of the incident within 24h. While the Commission starts from the proposition of the worst-case scenario to set a 24h reporting period to manage an incident that may have a global impact on other providers, it must also be considered that, should an incident occur in an entity, the company will first have to focus on mitigation measures and prevent any more damages in priority. The challenge to report in this short period of time also depends on the type of incident. Consequently, we deem urgent the need for a simpler and more pragmatic preliminary incidents notification system. In this respect, we suggest applying a standardized and user-friendly online reporting tool that allows entities to notify distinct institutions about an incident by sending encrypted messages and without generating subsequent queries from different sides. Additionally, it is essential, in our view, to have a single point of contact to handle the notification of incidents independently of the related sector, as well as a centralized platform to handle the different notifications of incidents. This is important in order to avoid confusion about what to report to whom. Furthermore, understanding and capturing the nature and the impact of the incident is the priority and the entity should work on the incident response first. Therefore, to be operational, our members recommend extending the period for reporting to at least 72h.

The proposed article 20 §2 of the NIS 2 directive imposes an **obligation to report both significant incidents and cyber threats**. However, we strongly believe that an information sharing mechanism for cyber threats would be more relevant and effective than a strict notification obligation. Indeed, not only is it difficult for companies to notify every potential cyber threat, but also would it be very difficult for authorities to receive and properly assess the notifications. Hence, the voluntary mechanism of sharing information about cyber threats would be more efficient. The large number of signals that could potentially lead to a cyber threat is not always appropriate nor relevant to be notified.

NOTE ON INFORMATION SHARING

Concerning cybersecurity-related information sharing for entities outside the scope of the proposed regulation (articles 26 and 27), FEDIL strongly encourages the voluntary approach. As cyber threats count among the information that can be shared between those entities, we believe it is worth considering expanding the cybersecurity-related information sharing to entities that fall into the scope of the proposed NIS 2 directive.

Furthermore, article 20 §3 proposes a **broad definition of the significance of an incident** and thereby leaves room for interpretation by the entity to evaluate the significance of an incident. Article 6 §1 of the current NIS directive sets some factors for determining the significance of a disruptive effect. To avoid any misinterpretation and misevaluation by entities, we would recommend highlighting such indicators to be considered by entities to determine the significance of an incident in accordance with the proportionality of the risks.

4. CERTIFICATION SCHEMES

Article 21 §1 proposes to give Member States the power to require essential and important entities to certify certain products, ICT services and ICT processes under specific **European cybersecurity certification schemes** adopted under the Cybersecurity Act. Although we support the certification mechanism to ensure the best quality of products, services and processes at European level, harmonization at EU level should be ensured in order to avoid that an entity could be obliged to certification in one Member State and not in another one.

Paragraph 2 proposes to give the Commission the power to adopt delegated acts to make certification mandatory. Yet, under the Cybersecurity Act, certification is applied on a voluntary basis, noting that several voluntary certification schemes that address security needs and identify relevant measures already exist[2]. To avoid contradictive cybersecurity legislation and ensure coherence, we would request to adopt the same voluntary approach in the NIS 2 directive. In addition, our members already apply a variety of ENISA or ISO cybersecurity certification schemes. To avoid redundancies, it should be verified whether the company already fulfils the conditions laid down in the new certification schemes via multiple other certifications already acquired: should all conditions be complied with, the company could be exempted from applying new certification schemes.

5. SUPERVISION AND ENFORCEMENT

As a preliminary note, our members observe that many provisions are the same for essential and important entities and only the supervisory regimes differ. For greater clarity and better legibility, companies would value one article on "*Supervision and enforcement for essential and important entities*" merging those provisions, specifying that they apply *ex ante* for essential entities and *ex post* for important entities. An additional article would lay down the specifying provisions which apply only to essential entities "*Additional supervision and enforcement for essential entities*". This would avoid redundancy and ease the reading of the text. Companies would have a better understanding of the common basis for all types of entities.

On the specific supervision measures, the proposal attributes specific powers to competent authorities, such as ***"on-site inspections and off-site supervision, including random checks"*** (article 29 §2 (a)). Concerning this new power, our members regret that the proposal does not give any precision on the frequency of checks by the competent authority. While we understand that the competent authority shall do its on-site inspections without warning to verify whether the entity is compliant with the new rules, other audits or requests shall be announced by a prior notification to the entities. More clarification on the occurrence and procedure of regular audits is needed. Indeed, it is very important for essential entities to prepare for such interventions as they will affect the companies' resources.

[2] Including but not limited to: ISO 27001 and 27000 family (ISO 27018, 27035,...), ENISA work products, NIST Cybersecurity Framework, 800-53, 800-171, FISMA, BSI 100-2 (IT Grundschutz), UK Cyber Essentials+, Cobit, SANS TOP 20 critical security controls, CIS Controls

POSITION PAPER

RESILIENCE OF CRITICAL ENTITIES

Competent authorities, where exercising their enforcement powers, will be able to order the implementation of ***"recommendations provided as a result of a security audit within a reasonable deadline"*** (article 29 §4 (f)). Our members agree that they have to comply with the new obligations but recall businesses always need a certain flexibility to continue running their activities. Entities should also be given the possibility to present their self-assessment to the competent authority which might adapt its order and deadline accordingly. Therefore, the "reasonable deadline" should be agreed with entities in order for them to be able to take the necessary actions according to the level of the risk they present. This would avoid setting a deadline within which entities could be facing a deadlock between remedying the issue or continuing delivering their services.

Furthermore, **some enforcement measures are overly restrictive and would not promote trust between entities and competent authorities**. The possibility of administrative fines shall be considered sufficiently coercive to ensure compliance with the proposed directive.

> FEDIL does not support article 29 §4, especially where competent authorities would have the power to ***"order those entities to make public aspects of non-compliance"*** (point (i)) and ***"make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation"*** (point (h)).
>
> In article 29 §5 (a) competent authorities shall have the power ***"to suspend a certification [...] concerning part or all the services or activities provided by an essential entity".*** This measure is disproportionate, especially considering that the deadline to remedy the deficiencies or comply with specific requirements shall be set by the competent authority.
>
> In article 29 §5 (b) competent authorities shall have the power to ***"impose a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity, and of any other natural person held responsible for the breach, from exercising managerial functions in that entity".*** This measure should be removed as it exceeds the usual liability for business related negligence and could result in personal liability. Indeed, article 17 §1 should be sufficient where it proposes to hold the management body accountable for non-compliance with the risk management measures.

It is important to engage with the entity to take the necessary actions according to the level of the risk it presents. We believe it is urgent to insert intermediary steps between the non-compliance, the possibility to seek remedies and such severe sanctions. For instance, competent authorities should request to act within a "deadline agreed". It is essential that entities and competent authorities cooperate in a coordinated manner and take into account the specificities of each company and the risk it represents.

These remarks also apply to the powers of competent authorities as regards supervision and enforcement measures imposed on important entities.

II. CER DIRECTIVE

Given the high level of interconnection among infrastructures, networks and operators delivering essential services across the internal market, FEDIL supports de European Commission's proposal for a directive to reinforce the resilience of critical entities. Although cybersecurity is not covered under the proposed CER directive, we believe regular exchange between regulators competent for the NIS 2 directive and CER directive is essential. Competent authorities need to adopt a holistic approach towards general resilience of critical and essential or important entities, they should address resilience as a priority and cooperate and communicate in a transparent manner. Our members welcome a closer alignment between the proposed CER directive and the services-oriented approach of the current NIS 2 directive to address the increased interconnectedness between the cyber and physical aspects of security.

Indeed, the operational environment of critical entities has changed significantly in recent years. The risk landscape has become more complex, as operators integrate new technologies such as 5G. Interdependencies between various operators grow and critical entities can potentially be affected by a disruption of a service provider active in another sector or another Member State of the EU. Hence, we strongly support the proposed directive's objective to increase the resilience of critical entities providing essential services to uphold the functioning of our society and economy as well as measures that will reduce the risk of the propagation of the effect of incidents on essential services in the EU. In this sense, FEDIL also supports the definition and establishment of specific rules of oversight for entities of particular European significance, which provide services in a large number of Member States. This will support resilience cross-border and in situations where a disruption could have a direct impact in various Member States.

Yet, we find it important to ensure that the CER directive does not introduce resilience requirements or reporting obligations on digital infrastructures, as they are indeed covered exhaustively under NIS 2 (in addition to DORA). Therefore, we ask for further clarification in article 7, read in conjunction with recital 14.

POSITION PAPER

RESILIENCE OF CRITICAL ENTITIES

A) IDENTIFICATION OF CRITICAL ENTITIES AND RISK ASSESSMENT

The current designation process described in the ECI directive by which Member States identify critical entities at national level is burdensome and led to inconsistencies in the internal market. We therefore welcome the risk-based approach laid down in the proposed CER directive.

According to the new proposal, **Member States will identify critical entities in specific sectors and sub-sectors** and establish a list to be updated when necessary. The directive specifies that this process should consider the outcomes of the risk assessment. The identification of critical entities shall take into account whether the entity provides for essential service(s), whether the service depends on an infrastructure located in the Member State and whether an incident would have significant disruptive effect (article 5 and 6).

Our members regret that the Commission did not provide for more transparency of this identification process. In practice, competent authorities could decide to keep this list of critical entities confidential. This would obstruct potential synergies within sectors and sub-sectors and, in turn, prevent from strengthening the resilience of the sectors. While keeping the list confidential would not prevent from further attacks, the actors on the market being a public information, making it public would support collaborations between entities from the same sector, facing the same risks. Moreover, making this information public is beneficial to customers and would enhance trust as identified entities will be shown to have a strong resilience and cybersecurity policy. Therefore, the proposed directive should include a provision to ensure full transparency on the identification of entities that are critical for the society. To allow entities to comply with their new requirements, we suggest making the list of identified critical entities public after a transition period of 2 years. Indeed, entities that have not been covered so far will need some time to prepare the implementation of the new directive.

As regards inconsistencies that could arise from the margin left to Member States in the identification of companies, we recommend that the European Commission develops guidelines or others instruments to reinforce the level of harmonization.

Further, an **obligation for critical entities to perform a risk assessment** has been laid down in the article 10 of the proposed CER directive. They will have to consider all relevant risks that may disrupt their operations and those referred to in the risk assessment to be done by Member States according to article 4. In particular, any dependency of other sectors of essential services, including those provided in another Member State or third country will have to be considered. Also, the impact that a disruption of the provision of essential services may have on other sectors or services provided by other critical entities will have to be observed.

While we agree with the necessity for critical entities to undertake a comprehensive risk assessment, it may be challenging for companies to fully assess their dependency risks, especially as regards the complexity of their downstream ecosystem. Therefore, we believe the responsibility should remain with competent authorities that are better equipped to be aware of potential dependencies as they have an overview of covered sectors. Once the dependencies have been determined, competent authorities could invite critical entities to provide them with the necessary information to complete the risk assessment in terms of dependencies.

Moreover, the directive proposes a period of 6 months as from their identification as a critical entity to fulfil their risk assessment. Our members regret that it will not be possible to conduct a risk assessment effectively in such a short time period. Once an entity has been identified as critical, a certain level of financial and human resources will have to be mobilized.

Especially, companies that are new to this process will have to first understand how and in what level of detail to carry out a risk assessment or they might have to invite external specialist to perform the risk assessment. These elements have to be taken into consideration when setting such a short deadline.

Alternatively, we would recommend that Member States set a list of identified risk that have to be assessed for each sector, including the public sector, and specifying which criteria have to be applied in the critical entities' risk assessment. Critical entities should not be requested to provide their risk assessment earlier than 12 months after the modality of the risk assessment and reporting have been defined. Extending the 6 months after identification to 12 months would be particularly useful to be included in risk treatment plans.

More generally, we would like to highlight that many actors of the sectors referred to in the Annex already carry out comprehensive risk assessments. For instance, in Luxembourg, critical entities already apply standards such as ISO 31000, risk management standards codified by the International Organization for Standardization. In the finance sector, support PSF entities have to fulfill Circular 12/544 [3] requirements on the "optimization of the supervision exercised on the "support PFS" by a risk-based approach" such as a yearly report on their risk management system and their self-assessment on the risks as regards the financial sector. Such circular precisely describes the content of the report and the risks to be assessed by entities. Since critical entities are already familiar with high level standards[4], FEDIL urges policymakers to adopt a more practical approach, in line with existing practices where entities would provide for a list of potential risks identified.

With regard to the identification of critical entities on the basis of their "**significant disruptive effect**", our members agree with the criteria to be considered according to article 5. Indeed, the number of users relying on the service (a); the dependency of other sectors (b); the potential impacts on economic and societal activities, the environment and public safety (c) etc. are all relevant criteria to define significant disruptive effects. Nevertheless, competent authorities will have to carefully transpose them as more details will have to be considered in practice. For example, some threats related to an incident might not yet show a significant disruptive effect although they could become very serious. It is therefore very important to describe principles on significant disruptive effect in detail at national level.

B) INCIDENT NOTIFICATION

Article 13 foresees those critical entities shall notify "incidents that significantly disrupt or have the potential to significantly disrupt their operations" to the competent authority without undue delay. While we acknowledge the necessity to notify incidents to avoid further damages across borders, we regret that no further details have been introduced as regards the notification procedure and the exact information that would need to be provided by the entity. Further, as it can be an immense challenge to assess the potential significance of an incident in terms of disruption, more guidance would be needed in this respect. To be more effective and reactive to significant disruptions, we believe that competent authorities, collaborating at EU level, should provide a list of typical scenarios to illustrate elements that need to be reported and provide guidance on what should be reported.

[3] https://www.cssf.lu/wp-content/uploads/files/Lois_reglements/Circulaires/Hors_blanchiment_terrorisme/cssf12_544eng.pdf
[4] For instance, ISO27001/ISO22301 - CSSF Circular 20/750

Essential service providers are requested to contribute to an overall national risk assessment including assessment of dependency risk. This assessment shall be updated on a yearly basis and managed by a public entity as information from different sectors and, in particular, of customers of service providers that the service provides may not be entitled to know, need to be combined.

C) COOPERATION

First, we welcome the proposed article 9 and that Member States shall facilitate cooperation and the voluntary exchange of information and good practices between competent authorities and critical entities. Overall, it is essential to provide support to critical entities in reinforcing their resilience since the services they provide are of vital importance for the society. We support the approach of the Commission which is pulling away from putting competent authorities in a supervision role only and push them more towards cooperation and support for critical entities.

Second, our members welcome the possibility given to the European Commission to support Member States and critical entities in complying with the new obligations by complementing the activities laid down in article 9. We also generally support the objective of strengthening capacities and improving cooperation as well as communication between stakeholders.

D) SUPERVISION AND ENFORCEMENT

In article 18 of the proposed CER directive, similarly than in the proposed NIS 2 directive, competent authorities would be allocated certain powers, means and responsibilities to supervise critical entities and enforce the new rules. For instance, it foresees the possibility to *"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"*. In line with our comments on the proposed NIS 2 directive above, our members regret that the proposal does not give any precision on the frequency of checks by the competent authority. For operators of critical entities to effectively allocate their resources, more clarification on the occurrence and procedure of inspections and audits is needed.

The proposal also foresees that the competent authorities may *"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"*. Consistent with our comments on the proposed NIS 2 directive, we believe the time period should not be unilaterally set by the competent authority but rather agreed on with the critical entities in order to take into account the different levels of complexity to remedy effectively to a potential infringement of the directive. We are in favour of an incident notification process that proportionate to the level of criticality.

Article 18 §2 (b) will give competent authorities the power and means to request "evidence of the effective implementation of {the new} measures, including the results of an audit conducted by an independent and qualified independent auditor selected by that entity and conducted at its expense". More clarification and guidance is needed on the evidence that could be requested and whether a certification or other framework would be appropriate documentation.

Finally, Member States will have to lay down rules on penalties applicable to infringements. We regret that the proposed directive does not provide for more guidance on the establishment of such penalties and leaves it to the Member States to determine different levels, which could potentially vary significantly within the internal market. We therefore recommend adapting the text and align it to the proposed NIS 2 directive where *ultima ratio* penalties have been proposed.