BUSINESSEUROPE

CYBERSECURITY ACT II

POSITION PAPER

WWW.BUSINESSEUROPE.EU

JULY 2026

KEY MESSAGES

01 A **unified EU approach to trusted ICT supply chains is preferable to 27 divergent national regimes** that would fragment the Single Market. However, harmonisation must not come at the expense of legal and investment certainty for businesses. **The framework needs stronger safeguards against legal and operational divergence to ensure consistent application and predictable conditions for cross-border business.**

02 **The effectiveness of the ICT framework hinges on legally robust design, particularly around the Commission's implementing powers and the delegation of politically sensitive decisions.** High-impact designation and restriction powers must be clearly grounded in Treaty-compatible legal bases, with safeguards ensuring compliance with Articles 290 and 291 TFEU to avoid legal and business uncertainty and legal challenges.

03 Mandatory phase-outs or forced replacement of ICT components can have far-reaching implications for industry, investment, business continuity, compliance costs and competitiveness. Such restrictions should only be used as a measure of last resort following a comprehensive, sector-specific risk and impact assessments, demonstrating that the benefits outweigh their economic and societal costs. Where such restrictive measures are adopted, a structured EU-level **compensation mechanism must also be put in place**, but compensation availability shall not be at the expense of robust and clear regulation.

04 Entities to be designated as high-risk, as well as EU critical infrastructure entities and integrating **companies, must be meaningfully involved before decisions are taken.**

05 **Certification should remain voluntary** to support innovation and SMEs and **operate alongside standards and other conformity routes** rather than as the sole compliance pathway. Industry should have an institutionalised role for regular input in certification development process.

06 ENISA's mandate should be measurable, and impact driven. **Clear KPIs are needed to assess performance,** including scheme uptake, operational effectiveness, and real-world improvements in EU cybersecurity posture.

07 The proposal as a whole **must strengthen Europe's global competitiveness,** avoid isolation from international standards, and ensure proportionate rules that do not undermine investment, trade, or cross-border operations.

08 The revised Cybersecurity Act (CSA2) should deliver meaningful burden reduction. New obligations under CSA2 must be assessed in light of existing requirements under NIS2 Directive, Digital Operational Resilience Act, Cyber Resilience Act, Critical Entities Resilience Directive, and other cybersecurity legislation to avoid duplication, legal uncertainty and unnecessary compliance costs.

CONTEXT

Over the years, BusinessEurope has consistently been engaged with the evolution of the EU cybersecurity framework. **We have advocated for a cybersecurity policy that is effective, proportionate, and supportive of innovation, competitiveness, and the functioning of the Single Market.**

A key principle underpinning BusinessEurope's positions has been that the role of the **European Union Agency for Cybersecurity (ENISA) should complement existing structures within the European cybersecurity ecosystem rather than duplicate activities** already carried out by national authorities, conformity assessment bodies, or standardisation organisations. Clear distribution of responsibilities across the European and national levels is essential to maintain regulatory clarity and ensure that efforts are focused where they bring the greatest value.

As regards certification and the general interplay of the Cybersecurity Act with other rules such as the Cyber Resilience Act, BusinessEurope has consistently highlighted the importance of building on the proven principles of the **New Legislative Framework.** This framework **demonstrates that harmonised standards, self-assessment mechanisms, and effective market surveillance can support a high level of safety in the Single Market.**

In this context, BusinessEurope maintains that cybersecurity certification should remain voluntary, affordable[1], and market driven. While certification can contribute to improving security and resilience, it should be viewed as one of several complementary tools within a broader cybersecurity framework.

The proposed **Cybersecurity Act 2 (CSA2)** represents a significant legislative instrument of the EU's cybersecurity architecture. We support the Commission's attempt to align the CSA2 with the Regulatory Fitness and Performance (REFIT) programme. We highlight, however, that the Regulatory Scrutiny Board (RSB) expressed in its opinion on the impact assessment several reservations with regards to burden reduction. The RSB further noted that the assessment of avoided costs and benefits must be improved, including by distinguishing between compliance and administrative costs. Any efforts to address these concerns during the negotiations should build on, rather than undermine, provisions that reduce administrative burdens and enhance legal certainty. In this respect, several elements of the proposal merit a particular support:

Voluntary Certification Framework: We strongly welcome that Article 71(3) maintains the principle that European cybersecurity certification shall be voluntary. This is preserving industry flexibility to demonstrate compliance with the best suitable option for the given business model.

Presumption of Conformity: The introduction of the presumption of conformity (Article 78) is a positive development, as it enables a single European certification to serve as sufficient evidence of compliance with relevant EU legal requirements, including frameworks such as NIS2 and the Cyber Resilience Act (CRA). **To ensure the organic uptake of certification among the entities operating in the EU Single Market, this mechanism should function as a simplification and burden reduction tool, whereby certification replaces, rather than merely supplements, detailed documentation and duplicative assessments.** For companies that choose to certify their cybersecurity posture, products, services, or processes under a European scheme, certification should be sufficient to demonstrate compliance and should not trigger additional national evidence requirements. At the same time, certification must remain strictly voluntary and should not, in practice, become a de-facto mandatory obligation through regulatory or public institutions' pressure.

[1] Certification may entail direct and indirect costs linked to product and organisational adjustments, documentation, tooling, preparation of auditable evidence, and third-party conformity assessment, depending on the scheme and assurance level.

Single Entry Point for incident reporting: the streamlining of incident reporting is crucial for entities to fulfil their obligations across multiple legislations. The "report once" principle should allow entities to fulfil overlapping reporting obligations through a single submission without establishing a centralised EU repository of incident data. A single point of submission and a federated information exchange system should be considered particularly during incidents when resources are strained, and businesses should not be required nor be put in a position to act as intermediaries between authorities. Clarifying and enforcing the principle of main establishment will be key in this approach.

Reinforced ENISA Mandate: Granting ENISA a well-resourced mandate (with an 81.5% budget increase) is vital for providing the stable expertise and capacity-building Member States and businesses require. Additionally, the early alert system for cyber threats, and the helpdesk against ransomware attacks, will directly help the awareness and swift actions of the economic operators. As ENISA's competences expand, it is important to ensure that its mandate continues to **complement in agile way, rather than duplicate,** national cybersecurity efforts or standardisation work at EU and international level. We therefore invite the co-legislators to consider clear key performance indicators (KPIs) to assess the effectiveness and efficiency of these measures, **ensuring that public funds are spent responsibly and that resources are deployed effectively** in line with our recommendations outlined below.

BUSINESSEUROPE'S RECOMMENDATIONS

TRUSTED ICT SUPPLY CHAIN FRAMEWORK (ADDRESSING NON-TECHNICAL RISKS):

While Title IV is based upon the supply-chain risk management framework established by NIS2 Directive, it also introduces a different regulatory approach. Unlike Articles 21 and 22 of the NIS2, which rely primarily on risk-based assessments by the entities and coordinated EU risk analysis, Title IV would empower the Commission to designate high-risk suppliers and third countries on the basis of non-technical criteria[2]. In doing so, legitimate business questions regarding its interaction with existing risk-management obligations[3] and the potential for regulatory overlap should be addressed. The political debate on these matters is timely and necessary to ensure substantial amendments to the proposed framework based on more comprehensive assessment of impact, costs and benefits and granting the legal certainty businesses need.

A harmonised approach to ICT Supply Chain security is preferable to avoid fragmentation in cross-border business operations within the Single Market. At the same time, while aiming for harmonisation the proposed Framework leaves the door open for fragmentation. Article 98(3) states that Member States may adopt or maintain stricter national measures, which creates a risk of gold-plating in the internal market. To achieve genuine Single Market harmonisation, Article 98(3) should be deleted, thus increasing the political importance of the common risk assessments.

Furthermore, BusinessEurope stresses the fact that legal acts, which restrict certain suppliers have far-reaching implications for investment, business continuity, cost of compliance and competitiveness,

[2] Irish Business and Employers Confederation (Ibec) considers that an enhanced role for Member States in the risk assessment and high-risk designation process is necessary to ensure that restrictive measures are imposed in strict, proportionate, clearly defined scenarios, once all other mitigation options have been exhausted.

[3] The Cyber Resilience Act aims to strengthen the security of products and services on the EU market, while the NIS2 Directive requires entities to manage supply chain and supplier related cybersecurity risks. Together, these frameworks are already driving a shift in market practices, purchases, and risk management approaches.

in general. Businesses need a stable framework to manage risks, plan investments, have confidence in their expected return on investment, and adapt their operations over time.

While several sectors had received previous indications of this direction of travel (e.g. de-risking and diversifying), for most sectors and entities identified in the NIS2 Directive this Framework will be a new approach. **We underline the observation of the Regulatory Scrutiny Board that the impact assessment of the proposal is not clear on the economic impact of replacement costs for ICT supply chain restrictions on the businesses in scope and downstream.**

One of the evident shortcomings of the ICT Supply Chain Framework is that its architecture relies on the assumption that complex and heterogeneous risks can be translated into **consistent policy outcomes across Member States** (Article 102 and 103). In practice, however, threat perception, intelligence inputs, and sectoral dependencies will vary significantly, across business operations and sectors, which makes uniform economic calibration of costs and benefits difficult. **Consequently, the assessments referred to in Article 103(4) should not be of a generalised nature.** Instead, they should be conducted separately for the sectors concerned and involve the relevant stakeholders in a sector-specific manner, ensuring that any mitigation measures subsequently adopted through legal acts are proportionate, technically appropriate, and feasible for the sectors to which they apply.

The harmonised approach sought under this proposal must not come at any cost or create legal and investment uncertainties for the businesses – significant questions remain regarding governance and practical implementation. The proposal needs to improve clarity on:

- **Legal foundation:** The limiting factors of existing toolboxes shall not only be attributed to the absence of binding rules, but also to the absence of a shared political agreement on threat perception and different levels of politically acceptable dependency. As argued above; by removing the possibility for national divergences under Article 98(3), the Framework becomes a stronger Single Market instrument, especially if the Regulation is to be based solely on that legal basis (Article 114 TFEU).
    - Considering that the objectives of the regulation are to address also the risks from foreign interference, adversarial cyber-attacks, espionage or campaigns against the Union or Member States, we would invite the co-legislators to consider whether exploring additional legal bases is going to strengthen legally the designation procedure and thereby the result from any restrictive actions taken under this regulation.
    - **Delegation of power:** The final stages of the designation mechanism in the proposal, in particular the power of the Commission to adopt implementing acts, raise questions in light of the Court of Justice's case law on the delegation of powers under Articles 290 and 291 TFEU. In a number of judgments[4], the Court has emphasised that provisions requiring political choices falling within the responsibilities of the Union legislature, or involving essential elements of a legislative framework, cannot be delegated to the Commission. Given that a high-risk designation may have significant consequences for market access, certification status, procurement eligibility, and the operation of critical services for the EU, it is not evident that such determinations can be characterised as purely non-essential implementing measures. We therefore encourage a further assessment by the co-legislators' legal services as to whether the proposed designation powers, the applicable criteria, and the resulting legal effects are compatible with the requirements of particularly Article 291 TFEU and the Court's case law. Without such legal certainty, the Framework may be susceptible to legal challenges from the affected parties and bring even further uncertainty on the business planning.
- **Mandatory prohibitions and costs:** The power to prohibit components from high-risk suppliers in relation to "key ICT assets" should be treated as an exceptional, last-resort measure, consistent

[4] Case C-355/10, Case C-270/12 (ESMA), Case C-427/12 (Biocides), and Case C-65/13 (EURES)

with the principles of proportionality and subsidiarity. **Priority should be given to less intrusive mitigation measures,** which must be realistic, technically and legally feasible, and take into account sector-specific operational constraints. Recital 144 acknowledges this to a certain extent, and it should be brought into relevant articles in CSA 2 Title IV Chapter I. Where phase-out or replacement measures would be imposed, these would constitute a significant interference with property and ownership rights and should therefore be strictly justified, risk-based, and accompanied by robust safeguards.

Additionally, such intervention could force enterprises to prematurely replace functioning equipment, generating environmental impact of disposing electronic "waste"; business continuity risks until replacement; cost volatility until an alternative is found; uncertainty how long the alternative will be deemed non-high risk, etc. While Article 103(4) rightly conditions the adoption of such measures on an assessment of the availability of alternative suppliers, that assessment should also consider whether those alternative suppliers ensure sufficient diversification. **The risks to the stability and continuity of essential and important infrastructure and services across the Union should not be overlooked.**

- **Scope clarification:** The trusted ICT supply chain framework, as described in Article 1(3), applies only to public or private entities listed in Annex I or II of Directive (EU) 2022/2555 that operate within the Union. **On a narrow interpretation, this may result in the framework applying only to EU-established manufacturers within the relevant Annex II sectors, while excluding comparable non-EU manufacturers placing products on the Union market.** In order to achieve the objective of resilience and security, the co-legislators therefore should clarify Article 1(3) to ensure that all economic operators placing products on the Single Market are subject to identical requirements under the trusted ICT supply chain framework.

  Furthermore, a differentiated approach could be examined where justified and aligned with the Union cybersecurity and cyber resilience objectives depending on criticality. For example:

  - For highly critical sectors (Annex I, NIS2 Directive), any restrictions could only be introduced where strictly necessary following a thorough risk assessment and applied as a last resort when less burdensome measures are insufficient. Implementation must ensure adequate transition periods reflecting practical constraints (including workforce, supply availability, and competing regulatory demands), continuity of service, maintained performance levels, and appropriate safeguards, including fair compensation, where relevant.
  - For other critical sectors (Annex II, NIS2 Directive), requirements could remain limited to forward-looking risk management. Proportionality should be ensured through grandfathering of existing products, systems, and equipment avoiding immediate compliance burdens under new rules.

  Furthermore, it must be recognised that recalling products from the Single Market solely because a component has been designated as high-risk asset would cause severe disruption of the Single Market architecture, particularly with regard to logistics, economic activity, and business continuity. **Market Surveillance Authorities and their expertise must also be brought into the cross-authority cooperation obligations of ENISA.**

- **Compensation scheme:** To address the financial consequences of mandatory replacement or forced phase-out, a European-level compensation mechanism should be established. This would cover damages where ICT components are still within their technical lifespan, recognising that such costs are not commercially driven but arise directly from public policy choices linked to geopolitical or strategic objectives. In effect, impacted companies are bearing costs that serve collective security objectives rather than market-based decisions, reinforcing the need for proportionate design and fair burden-sharing. At the same time, the potential availability of compensation should not serve as a substitute for proportionate and evidence-based regulation.

Any compensation mechanism should be accompanied by robust governance safeguards to ensure that it remains an exceptional tool.

- **Corporate oversight:** Ownership and control criteria should be grounded in demonstrable cybersecurity risk and linked to clear, measurable cybersecurity outcomes. Requirements should therefore be proportionate, risk-based, and avoid duplicative compliance across jurisdictions or unintended barriers to international operations.

  Additionally, "control" should be defined as concretely as possible in the main text, for example, considering majority ownership (by third country nationals), state ownership, legally binding authority to direct corporate decisions, or formal governance rights that enable decisive influence over security-relevant choices. The definition should avoid unintentionally capturing globally operating companies with diversified ownership structures and limited exposure to the identified cybersecurity risk.

- **Impact:** A thorough assessment weighing the economic impact on procurement costs[5] and consumer prices resulting from high-risk supplier restrictions could help track the proportionality of the intervention. The impacts on trade (e.g. counter measures by the designated third country), digital decade ambitions, the environment, customers and service-users, and long-term EU competitiveness, including the impact of energy costs[6], must also be considered.

- **Thresholds for actions:** Article 99 stipulates that coordinated EU-level security risk assessments must be completed within six months by the NIS Cooperation Group and such can be initiated by the EU Commission or a minimum of three Member States. However, the third paragraph of the article is based on "sufficient reason to believe" a significant cyber threat exists, which may give the initiation threshold considerable flexibility, and potentially leading to frequent or rapid activation of the assessment mechanism by the EU Commission (Article 99(3)(b)). Furthermore, it is not clear via what channel would the European Commission receive any knowledge of imminent threat to essential and important entities, given that the EU Commission is neither tasked nor expected to be the holder of such crucial cyber intelligence information. This provision is not grounded on the architecture of cyber-information and intelligence exchange under the existing regulations.

- **Thresholds for triggering risk verification:** Article 100 points that a single member state can trigger a verification of the risk from a third country by the Commission, whereas three member states can initiate a risk assessment under Article 99. It reads as if Article 100 is not strictly dependent on the coordinated risk assessment, thus reducing its necessity, considering that the Commission can act based on intelligence from other sources, or public statement by one member state.

  - The low threshold of one Member State asking the Commission to verify the risk posed by a third country risks politisation of claims in a geopolitically unstable environment. In any case, an initiation of a verification would be already alarming for businesses, dampening investment intentions or triggering new search for alternative suppliers, even if the verification is inconclusive or concludes that there is no risk. Article 100 needs to be amended in a way that it safeguards against one-country setting the EU agenda for political or domestic reasons and keep the speed element without undermining the value of coordinated risk assessment under Article 99.

[5] The revision of the public procurement directives should be taken into consideration. See BusinessEurope reply to the consultation.

[6] See the study on Energy and Climate transition commissioned by BusinessEurope, showing that even in the case of a managed transition, with more supportive EU energy policies, energy costs in Europe would be at least 50% higher than in the US, China and India by 2050.

Restrictions regarding key ICT assets should only be considered after a thorough assessment of available mitigation measures under Article 103(2) and where such measures have demonstrably proven insufficient. Any restrictive measures should therefore constitute a measure of last resort, supported by a sector-specific assessment of necessity, proportionality, feasibility and economic impact.

- **Transparency and dialogue:** The procedural safeguards provided for in Articles 104(4), 105 and 106, including the opportunity for affected entities to provide information and exercise their right to be heard, are important and should be preserved. In addition, the implementation of these provisions should ensure that the specific circumstances of suppliers and entities are appropriately considered, including whether effective risk-based mitigation measures or an exemption could address the identified concerns before the most restrictive measures are applied.

EUROPEAN CYBERSECURITY CERTIFICATION FRAMEWORK (ECCF)

We welcome the clarification that schemes should include only technical criteria for assessing the assurance levels of the entities applying for a certificate. We reiterate that BusinessEurope considers that cybersecurity certification should remain voluntary, affordable, and market driven. However, below are several problematic provisions that we would like to see improved.

- **Self-certification:** While industry advocates for self-assessment to maintain speed-to-market, **the proposal restricts conformity self-assessment strictly to the "basic" assurance level,** potentially increasing costs for medium-risk innovative products. It is unclear how this proposition in the Cybersecurity Act 2 is in line with the scope of the Cyber Resilience Act (CRA), where the risk assessment of the products dictates what type or requirements will be implemented and they may not be listed as important Class II or critical under the CRA. In other words, the CRA allows self-assessment only under strong conditions (scheme or standards applied, Article 32 (2)), while the CSA2 associates self-assessment with basic assurance. Furthermore, the AI Act, has the option to undergo internal control conformity assessment even for high-risk products (article 43). Hence, the proposal must be aligned with other Union law.

- **Challenging default timeline for schemes development:** A 12-month deadline for ENISA to prepare candidate certification schemes appears too restrictive and could negatively affect the quality of the work delivered. Compressing its timeline risks limiting proper technical development, and stakeholder participation, particularly for schemes that cannot build upon existing frameworks, or standards. A 24-month timeframe would therefore be a more balanced and realistic approach.

- **Cyber posture scheme:** Cyber posture certification can help reduce administrative burdens but must remain strictly voluntary for NIS2 entities. It should not become a mandatory centralised supervisory mechanism. Standards or alternative means of demonstrating NIS2 compliance should be explicitly recognised in the main text considering that compliance assessments for NIS2 Directive remain the responsibility of national competent authorities.

- **Bypassing standardisation organisations:** Article 77 and 81 allow ENISA to draft technical specifications when international standards are deemed missing or not suitable. There appears to be a certain conflict of interest as ENISA who will be drafting the schemes will also help the Commission assess if other ways to demonstrate compliance (i.e. via harmonised standards) are fit for purpose, which gives the Agency the power to turn down standardisation which usually is the preferred industry-driven option. We are concerned this could lead to European isolationism, moving away from the global consensus-based standards that companies would need to rely on in order to scale beyond Europe's borders.

- **Fees:** The introduction of a power for ENISA to levy fees for maintaining certification schemes and using testing tools adds a new financial burden for businesses that are already facing significant compliance costs. In addition, the relationship between these new fees and the

estimated reduction of EUR 14 billion in costs mentioned in the Impact Assessment remains unclear. There is therefore a certain irony in the proposed system where companies are expected not only to invest in implementing cybersecurity requirements, but also to contribute financially to the mechanisms designed to test their compliance, while already supporting the broader public policy framework and ENISA's funding through general economic contributions. **These fees should therefore be eliminated, as they would have adverse consequences for MSME participation and they contradict the stated objectives of the CSA2 regarding burden reduction** Instead, consideration should be given to establishing financial incentives for MSMEs to address the costs that may arise if certification schemes become more widely required.

- **Engagement with industry stakeholders:** Meaningful stakeholder engagement is another key element of an effective European cybersecurity policy. While the Stakeholder Cybersecurity Certification Group (SCCG) established under the old Cybersecurity Act was not functioning in a satisfactory manner, the removal of such an accountability-relevant group is an alarming signal. Instead, the operation of such a group could have been improved, while also introducing the ad-hoc exchange possibilities in CSA2. In this context, it would be important that Regulation specifies the categories of stakeholders to be represented in the Assembly, rather than relying solely on an open-ended reference to "relevant stakeholders" or "relevant experts".

    - Industry expertise plays an essential role in the development of workable cybersecurity measures and certification frameworks. Consultation mechanisms should therefore ensure structured and substantive participation of stakeholders throughout the policy development and implementation process. Engagement should enable genuine dialogue and allow stakeholders to contribute technical knowledge and operational experience, ensuring that outcomes are practical and implementable for organisations across sectors. To further improve transparency and predictability, ENISA should be required to publish and regularly update an action plan for the development and maintenance of schemes, including key milestones and consultation timelines. Moreover, ENISA and the Commission should publish summaries of stakeholder feedback received during feasibility studies, scheme development, and maintenance, and clearly explain how such input has been taken into account in subsequent revisions.

    - The Stakeholder Cybersecurity Certification Group should be reinstated, and its modus operandi improved (e.g. including by having joint discussions with the ECCG on matters related to the business impacts of schemes; receiving questions to be discussed upon the documentation, to avoid "broadcast-like" meetings with limited interactions).

BURDEN REDUCTION OPPORTUNITIES AND MARKET FRAGMENTATION RISKS:

- **Security objectives:** The objective of reducing compliance costs should also be assessed in light of the level of prescriptiveness introduced by the framework. With more than twenty cybersecurity objectives in Article 80, the approach risks becoming highly detailed, potentially limiting flexibility and agility of the (future) schemes development. Having objectives listed in the main text (as it transpires) based on pre-conceived ideas of what schemes will be developed in the short-term is counter to the idea for a long-term regulatory certainty and stability. Therefore, the security objectives need to be revised in light with their long-term applicability. Moreover, a number of these objectives replicate obligations already established under other frameworks, such as the CRA and NIS2, leading to overlap and possible inconsistencies. Unlike the CRA, which sets out clearly risk-based objectives in Annex I Part I (2), Article 80 defines its goals in absolute terms and does not take proportionality or risk into account. Article 81 shall be similarly streamlined. This is necessary, since the CRA and NIS2 already establish horizontal cybersecurity and product security requirements across the EU economy, any additional measures should be carefully assessed to avoid duplication and ensure proportionality.

- **Penalties:** While high penalties are justified to deter deliberate non-compliance, their apparent calibration to very large companies may lead to disproportionate impacts on smaller entities, raising concerns regarding proportionality. In addition, the magnitude of potential sanctions may have a chilling effect on smaller companies' willingness to engage in new business models or to cooperate in regulatory processes, particularly where repeated exposure to significant penalties over time could materially affect their viability.

- **Requirements mapping:** We invite the European Parliament and the Council of the European Union to carefully avoid adding new or overlapping requirements, and instead prioritise the development of a comprehensive mapping between CSA2 and existing EU and sectoral frameworks (NIS2, DORA, CER Directive, DNA, etc). This would contribute to a more coherent and workable regulatory framework for all sizes of companies affected, while helping limit the administrative burdens.

ENISA'S MANDATE

Ensuring that ENISA remains a technically driven agency with a clear mandate, a complementary relationship with national authorities, and a strong framework for stakeholder engagement will help maintain a coherent and effective European cybersecurity architecture that benefits both public authorities and the broader European economy. add Some further changes would be required to help keep the technocratic mandate of ENISA:

- **ENISA Advisory Board:** While it is positive to have a broad participation of stakeholders in the Advisory Board, limiting its remit to deliver feedback on ENISA's tasks as provided in Article 35(5) is already a signal that the Advisory Board would not be a place for a well-rounded discussion on strategic priorities for the cybersecurity ecosystem of Europe.

- **Non-binding nature:** ENISA's technical assessments must remain non-binding and shall not override national security competencies of Member States authorities.

- **Personnel vetting procedures:** ENISA will be increasingly receiving sensitive business information and data regarding ransomware, incidents or vulnerabilities faced by the entities in Europe. Without questioning the necessity of adequate staffing we also underline that the vetting procedures must be robust to avoid risks of infiltration or confidentiality breaches.

- **Support in incident response:** As ransom attacks are a type of crime that law-enforcement authorities are dealing with, the ENISA helpdesk must not lead to any confusion as to who is "in charge" to investigate and help the attacked entity. The operationalisation of the cooperation with Europol therefore is essential (currently, Recital 37 is ambiguous). Ransomware attacks are among the most visible and disruptive ways in which companies experience cyber threats in practice, often translating abstract cybersecurity risks into immediate operational and financial harm. As such, **they are a critical test case for the effectiveness of the EU's cybersecurity framework.** Any lack of clarity or coordination in the institutional response risks undermining trust and creating a perception of fragmentation at EU level, underscoring the importance of a well-organised and clearly communicated approach. Co-legislators should organise a structured exchange ahead of the adoption of their respective negotiation positions in order to clearly define roles, responsibilities, and coordination mechanisms, and to ensure a clear distinction between advisory support (ENISA) and law enforcement functions.

- **Key performance indicators** can be introduced in the main text to ensure that its objectives are actively monitored; for example, certification velocity for entities; measuring the workforce mobility via the portability of the skills attestation; measuring year-on-year the number of valid certificates (re)issued and the share and relative costs of MSMEs obtaining them; tracking the ransomware attacks and the recovery time; monitoring the number of entities with cyber posture

certificates to demonstrate compliance across the cyber legislation. In addition, KPIs can be extended to enhance ENISA's visibility and operational impact towards essential and important entities by measuring the timeliness and reach of shared cybersecurity situational awareness outputs under Article 11, 12 and 13 (including dissemination latency and entity coverage; responsiveness and uptake of early alerts, including alert delivery speed, penetration across NIS2 Annex I and II entities, and the extent to which alerts lead to preventive mitigation actions.

BUSINESSEUROPE

BusinessEurope is the leading advocate for growth and competitiveness at the European level, standing up for companies across the continent and campaigning on the issues that most influence their performance. A recognised social partner, we speak for enterprises of all sizes in 36 European countries whose national business federations are our direct members.

Austria | Belgium | Bulgaria | Croatia | Cyprus | Czech Republic

Denmark | Denmark | Estonia | Finland | France | Germany

Germany | Greece | Hungary | Iceland | Iceland | Ireland

Italy | Latvia | Lithuania | Luxembourg | Malta | Montenegro

Norway | Poland | Portugal | Rep. of San Marino | Romania | Serbia

Slovak Republic | Slovenia | Spain | Sweden | Switzerland | Switzerland

The Netherlands | Türkiye | Türkiye | Ukraine | Ukraine | United Kingdom

Avenue de Cortenbergh 168
B - 1000 Brussels, Belgium
Tel: +32(0)22376511 / Fax: +32(0)22311445
E-mail: main@businesseurope.eu

WWW.BUSINESSEUROPE.EU

EU Transparency Register 3978240953-79