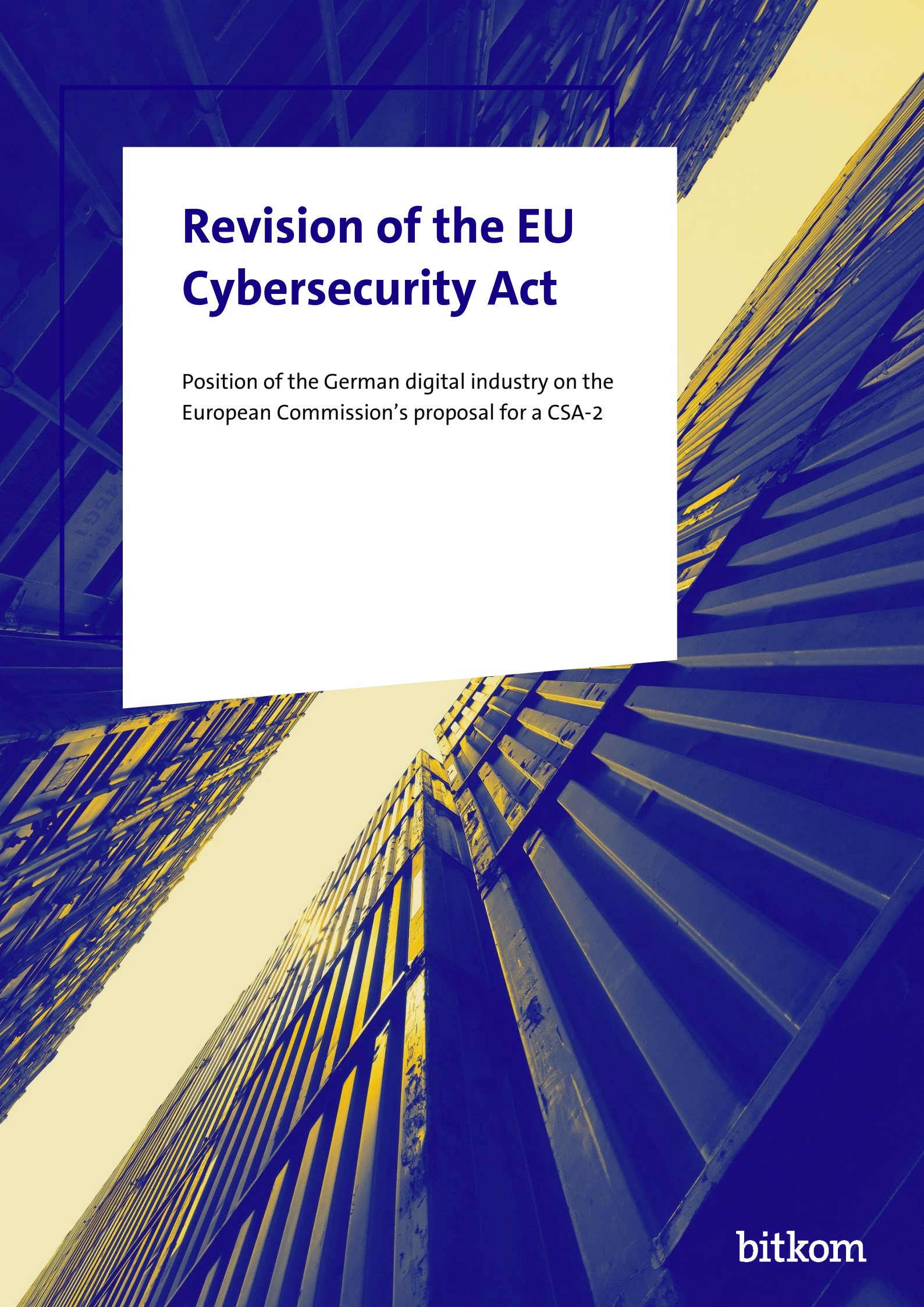

Revision of the EU Cybersecurity Act

Position of the German digital industry on the European Commission's proposal for a CSA-2

bitkom

Content

1 Summary 3

2 TITLE II: THE EUROPEAN UNION AGENCY FOR CYBERSECURITY 5

3 TITLE III: EUROPEAN CYBERSECURITY CERTIFICATION FRAMEWORK 8

Article 71: Objectives and scope of the European cybersecurity certification framework 9

Articles 72–74: Stronger and more binding stakeholder engagement in the development of certification schemes 10

Article 74: Transparency and traceability in the scheme drafting process 10

Articles 75–76: Maintenance and evolution of certification schemes 10

Article 78: Presumption of conformity as a tool to support regulatory compliance 11

Article 80: Security objectives of European cybersecurity certification schemes 11

Article 81: Elements of European cybersecurity certification schemes 12

4 TITLE IV: SECURITY OF ICT SUPPLY CHAINS 13

Article 99: Security risk assessments 15

Article 100: Designation of third countries posing cybersecurity concerns 15

Article 102: Identification of key ICT assets 16

Article 103: Mitigation measures in the ICT supply chain 16

Article 100(4): Consequences of designation 17

Article 104: Identification of high-risk suppliers 17

Article 105: Exemption for entities established in or controlled by entities from a third country posing cybersecurity concerns 18

Article 115: Penalties 19

Chapter II: ICT supply chains in electronic communications networks 19

1 Summary

The initial focus of the Cybersecurity Act (CSA) from 2019 was strengthening the mandate of the EU agency ENISA (EU Agency for Cybersecurity) and creating the European Cybersecurity Certification Framework (ECCF) for the voluntary certification of ICT products, services and processes. In the meantime, however, the regulatory landscape has evolved significantly: With the Network and Information Security Directive 2 (NIS-2), the Digital Operational Resilience Act (DORA), the Cyber Resilience Act (CRA), and the Radio Equipment Directive Delegated Act (RED-DA) and cybersecurity parts of the AI Act and the new EU Machinery Regulation, a large number of other regulations have come into force with partially overlapping requirements or are about to be implemented. Companies are confronted with parallel reporting obligations, different national implementation practices and regulatory duplication. This threatens to reverse the goal of a resilient digital infrastructure: Security is not created through complexity, but through impact.

The Cybersecurity Act 2 (CSA-2) proposal aims reform ENISA, improve the ECCF, and strengthen Europe's ICT supply chains. Bitkom is clearly in favour of a targeted revision towards a CSA-2. This includes strengthening ENISA as the central authority for technical implementation aids for NIS-2. Equally important is a paradigm shift in the certification process: Certification must remain voluntary. The procedures must be made more transparent and accessible, stakeholders must be more broadly involved, and certification schemes must be limited to technical criteria. Current practice, as in the case of the EUCS scheme, clearly shows the weaknesses of the existing model: a lack of transparency, a lack of official drafts and the influence of geopolitical considerations are blocking progress.

Title IV of the CSA-2, which introduces a trusted ICT supply chain framework, addresses an important objective: secure and reliable ICT supply chains are essential for the functioning of critical services, the Single Market, and society as a whole. Bitkom therefore supports the aim of strengthening Europe's resilience against external shocks and undue harmful influence by third countries. However, such a framework must be legally sound, proportionate, and operationally workable. Additional obligations must be complementary and not undermine existing rules, especially where instruments such as the GDPR already address relevant risks, provided they are implemented and enforced consistently. In this regard, a harmonised EU-wide approach consistent with the EU's simplification agenda should take precedence over fragmentation and avoid unnecessary gold-plating, while building on and not contradicting existing national security decisions adopted at Member State level. To ensure coherence and effectiveness, this approach should rely on coordinated EU-level risk assessments, be developed with structured involvement of relevant industry stakeholders, and remain sufficiently flexible to account for the specific risk profiles of different sectors. Given the far-reaching implications for affected industries and supply chains, the framework requires a clear legal basis, meaningful Member State and stakeholder involvement. It is questionable whether an Implementing Act is the appropriate instrument for such measures. Where restrictive measures are imposed in

59%

of all German companies consider cyberattacks to be an existential threat. (Bitkom, 2025)

the public interest, their practical and economic effects must remain proportionate and should not shift uncompensated costs to affected companies and customers.

Furthermore, it should be clarified how the entity-based scope of CSA 2 is intended to operate in practice and whether it creates regulatory asymmetries. Since CSA 2 mirrors the entity-based logic of the NIS-2 Directive, which focuses on activities carried out within the EU, its scope appears to cover organisations that are established in the Union and conduct relevant activities there. In practice, this would mean that CSA 2 applies to service providers covered by Annex I of NIS-2 and to organisations such as manufacturers covered by Annex II of NIS-2, provided that they are established and operating in the EU. By contrast, products manufactured outside the EU by entities that do not themselves fall within the scope of NIS-2 may remain outside the CSA 2 framework where they are merely placed on the EU market. This would create an uneven playing field and a competitive disadvantage for entities with manufacturing operations in the EU, particularly when supplying EU entities that are not listed in Annex I of NIS-2. Therefore, entities covered by Annex II(5) of NIS-2 are to be exempted from the scope of the CSA-2.

The CSA-2 should also respond to a closely related but broader problem: the growing complexity caused by overlapping cybersecurity legislation, particularly between the NIS-2 Directive and the CRA. As it stands, NIS-2 will be revised and simplified through a proposed draft directive, which Bitkom is covering in another position paper. In contrast, the CRA is not encompassed by the current simplification efforts, despite evident inconsistencies with other legislative instruments. NIS-2, the CRA and other legislations establish largely identical incident reporting timelines, yet rely on separate procedures and responsible entities, potentially leading to up to six parallel reports for a single cybersecurity incident. EU legislation should consistently adhere to the principle of «one incident, one report, one reporting mechanism/format, and one reporting point», extending beyond the concept of a single reporting platform as envisaged in the Digital Omnibus. To this end, a clearer delineation of reporting obligations, harmonised definitions across various legal acts, and corresponding adjustments to ENISA's mandate are required.

Finally, Bitkom would like to recall the European Commission's stated objective of the CSA-2 in the spirit of regulatory simplification. In the public consultation, the Commission emphasised that the review represents «an opportunity to further simplify cybersecurity rules» by streamlining reporting obligations, facilitating implementation, reducing administrative burdens and fostering a business-friendly environment. Against this backdrop, the current draft with 270 pages of new or amended provisions raises concerns. Both its scope and a number of substantive requirements risk running counter to the stated goal of simplification, as they introduce more obligations and compliance efforts for companies.

Before turning to the details of the CSA-2, Bitkom therefore stresses a general point: the CSA-2 must remain true to its core objective of simplification and coherence. It should streamline and consolidate existing requirements rather than establish another complex legislative framework that increases administrative burdens without delivering commensurate gains in cybersecurity.

2 TITLE II: THE EUROPEAN UNION AGENCY FOR CYBERSECURITY

ENISA should not only be an advisory body but rather become a central operational hub. Both the NIS-2 Directive and the CRA assign ENISA a substantial number of new responsibilities, which require consistent implementation and coordination at the European level. Under the NIS-2 Directive, these tasks include the development and maintenance of registries for vulnerabilities and cross-border services, the coordination of best practice sharing among Member States and within the European Cyber Crises Liaison Organization Network (CyCLONe), as well as the annual reporting on the state of cybersecurity across the EU. Building on these expanding responsibilities, within the CRA, ENISA is likewise assigned several key responsibilities such as the operation of the reporting platform.

Bitkom welcomes the mandate in Article 15 to develop it into a single reporting platform; however, it is essential that the CSA-2, NIS-2, CRA, GDPR, DORA and AI Act are adapted and aligned to state that a single report to ENISA fulfils all reporting obligations for that incident. Furthermore, the CSA-2 should explicitly prohibit Member States from imposing additional reporting obligations for the same incident to ensure true standardisation. National authorities must be required to connect to the ENISA platform to prevent fragmentation, as the current omission of DORA and GDPR in Article 15, and the lack of amendments to Article 23 of NIS-2, threatens the effectiveness of this centralised approach. Moreover, ENISA should be tasked with developing best-practice guidelines that consolidate Member States' approaches to incident handling and apply the once-only principle – ensuring incident information is reported once and reused securely across authorities.

Building on this need for regulatory alignment, the increasing number of horizontal and sectoral regulatory requirements related to data access and data sharing must be carefully assessed from a cybersecurity perspective. While additional mandatory interfaces for data sharing may create value for data recipients, they can also significantly weaken the cybersecurity of devices or even conflict with existing cybersecurity legislation. In this context, ENISA should be mandated to carry out a mandatory «cyber proofing» of all EU legislation that introduces data-sharing obligations, in order to independently assess whether such provisions may introduce or even legally require the disclosure of cybersecurity vulnerabilities.

In addition, clarity is needed regarding the interaction between ENISA's early warning functions and existing EU frameworks for vulnerability reporting and coordinated disclosure. Where ENISA issues early warnings on cyber threats or vulnerabilities, such alerts should be limited to vulnerabilities that are already publicly known and must not interfere with ongoing responsible disclosure or mitigation processes, in particular those established under the CRA. Premature or uncoordinated disclosure of sensitive vulnerability information could otherwise undermine trust in reporting mechanisms and increase systemic risk. Vulnerabilities reported under the CRA should not be

considered «publicly known» solely by virtue of having been reported, particularly where mitigation or coordinated vulnerability disclosure is ongoing.

ENISA should coordinate national market surveillance to ensure a level playing field for all market participants under EU cybersecurity law. This new responsibility requires a dedicated increase in the agency's personnel and financial resources to ensure effective implementation. While Bitkom supports a strengthened operational role for ENISA, it is equally essential to maintain a clear distinction between implementation support and standard setting. In particular, where ENISA is tasked with developing technical specifications to support Union law or certification schemes, this should not result in ENISA acting as a de facto standardisation body. Consensual international standards developed in recognised standardisation organisations, in line with WTO TBT principles, must remain the primary reference. ENISA's role should focus on facilitating implementation, consistency and interoperability, without replacing or duplicating established international standardisation processes, including in sensitive areas such as cryptography. With regard to emerging technological challenges such as post-quantum cryptography, ENISA's role should likewise be clearly delineated. While it should build technical expertise and contribute to evaluation and coordination, its activities should remain complementary to established international and European standard-setting processes. ENISA should not develop or approve cryptographic standards independently, but support internationally recognized processes to ensure interoperability, consistency and trust in the global cryptographic ecosystem.

At the same time, ensuring the practical success of these frameworks also requires addressing financial barriers. To ensure broad uptake of European cybersecurity certification schemes, the cost-recovery approach set out in Articles 46 and 47 should be reconsidered. Requiring ENISA to charge manufacturers and conformity assessment bodies for certificates and technical tools creates financial uncertainty and additional administrative burden for companies. Unpredictable EU-level fees make compliance budgeting more difficult and risk discouraging participation in certification schemes. This is particularly problematic as cybersecurity certification serves a clear public interest by strengthening resilience and trust in the digital ecosystem. The certification infrastructure could therefore be financed through public funds in addition to levies on market participants. Compensating some fees would support wider adoption and ensure that financial uncertainty does not hinder efforts to enhance Europe's cybersecurity level.

Finally, alongside adequate resources and accessible certification structures, the active and continuous involvement of industry stakeholders is essential to ensure that cybersecurity certification schemes evolve in a sustainable, practical, and technically robust manner. Bitkom recommends the establishment of structured non-discriminatory Public-Private Partnership models and particularly welcomes the ENISA Advisory Group as defined in Article 35, notably its strong industry representation and the rotation procedures that ensure a broad influx of expertise. To ensure this collaborative approach is effective, the guidance provided by the Advisory Group must be systematically taken into account by ENISA's Management Board and Directors. Furthermore, the CSA-2 should explicitly expand ENISA's mandate to cover ongoing scheme maintenance, ensuring the agency is equipped with the necessary financial and human resources to fulfil this role in close alignment with industry know-how and EU strategic objectives. While the CSA 2 rightly strengthens ENISA's role in

international cooperation, it should be clarified that ENISA's engagement with industry experts and private sector partners must remain open, as access to global cybersecurity expertise and threat intelligence is essential for effective risk mitigation and situational awareness.

3 TITLE III: EUROPEAN CYBERSECURITY CERTIFICATION FRAMEWORK

The proposed update of the CSA-2 addresses three central shortcomings of the current ECCF: slow scheme adoption, overly complex governance and limited market uptake. Bitkom welcomes the intended repeal and redesign of the ECCF, including the clearer timeline for ENISA to draft schemes, the introduction of mandatory maintenance and review mechanisms, and the stronger emphasis on transparency and structured stakeholder involvement. In particular, the proposed alignment with NIS-2, the CRA, the GDPR and other relevant Union legislation is an important step to ensure that certification supports regulatory coherence rather than creating additional complexity. At the same time, certification schemes under the ECCF should remain strictly technical in nature.

A key improvement is the reinforced role of certification as a presumption of conformity. Cybersecurity certification schemes under the ECCF can strengthen legal certainty and ease the burden of proof under horizontal and sector-specific rules, including NIS-2, DORA and the CRA, while reducing administrative and compliance costs. To deliver these benefits, European schemes must contribute to simplification and market unity. Diverging national schemes and interpretations currently fragment the market; Member States should therefore refrain from introducing parallel national certification schemes or additional regulatory layers in areas already covered by an EU scheme. At the same time, European certification should be designed to complement broader efforts and sector expertise, including industry-led initiatives such as the Network Equipment Security Assurance Scheme (NESAS), which can support practical implementation and international alignment.

International interoperability is also decisive for market uptake. EU cybersecurity certification schemes should align closely with established international standards, including ISO 27001 and TISAX, and should allow for the reuse of existing European and international standards rather than duplicating them. Avoiding isolated EU-specific requirements helps prevent market barriers, strengthens European companies in global competition and supports acceptance beyond the EU. The proposed Article 87 on the international recognition of European cybersecurity certificates, and vice versa, provides a constructive basis to operationalise this objective and should be leveraged to enable credible recognition pathways.

While the proposal rightly seeks to accelerate scheme development, the pace of adoption under the ECCF remains a structural concern. Bitkom therefore supports focusing schemes on technical requirements as a means to improve feasibility and speed. However, quality and market relevance must be safeguarded through formal opportunities for stakeholder input throughout the drafting process, particularly when substantial changes to an initial draft are considered. In this regard, the proposed 12-

month deadline for ENISA to draft new schemes may be overly ambitious; an 18-24-month timeframe appears more realistic if the process is to deliver schemes that are technically robust and usable in practice. In addition, existing certifications should remain valid until the new framework is fully in place, as premature invalidation would risk forcing companies into individual solutions and undermining continuity.

Finally, clarity is needed on the scope of schemes, including a consistent distinction between services and products. As a rule, schemes under the CSA-2 should focus on services. Where schemes also cover products, they should be fully embedded in existing conformity assessment procedures under relevant Union harmonisation legislation, such as the CRA, the MDR or other New Legislative Framework instruments, and should not establish parallel or stand-alone assessment regimes. Overall, certification should remain a strictly voluntary instrument that incentivises compliance and facilitates market access, while remaining coherent with standardisation initiatives already underway in recognised bodies.

Against this background, Bitkom sees a need to further clarify the objectives and scope of the ECCF to ensure coherence, proportionality and alignment with international standards, and to avoid unnecessary regulatory burdens.

Article 71: Objectives and scope of the European cybersecurity certification framework

Bitkom supports the development of a common cybersecurity certification scheme under the European Cybersecurity Certification Framework (ECCF). In light of existing schemes such as BSI-NESAS, BSI-BSZ, the EU-CC certification framework, and comparable certification systems in other Member States, the ECCF must ensure harmonization, cross-Member State acceptance, and significantly reduce the risk of duplicate certification efforts.

At the same time, the wide range of already established standards and certification schemes must be duly recognized and systematically taken into account within the European certification process. Rather than reinventing the wheel, the EU should build on proven international standards such as ISO/IEC 27001 and TISAX, which are globally recognized, widely implemented, and effective in practice. Introducing a new European scheme must avoid creating redundant parallel structures or imposing additional evidence requirements on companies that already hold equivalent certifications, as this would increase administrative burden without delivering measurable cybersecurity improvements. Until the new ECCF scheme is fully in force, Member States should immediately recognize certifications granted in other Member States for defined products and processes in order to prevent fragmentation and unnecessary double efforts.

In addition, cyber posture certification should be designed in a proportionate and risk-based manner, focusing on those services, assets and organisational units that fall within the scope of NIS-2 rather than being applied by default at the level of the entire organisation. Companies should also retain maximum flexibility in how they demonstrate compliance, whether through a future cyber posture certification scheme or through separate audits conducted by national regulators.

Articles 72-74: Stronger and more binding stakeholder engagement in the development of certification schemes

Bitkom welcomes that the draft acknowledges the importance of public information and consultation in the certification process. To ensure that stakeholder engagement effectively contributes to the quality and practicality of certification schemes, the certification process should be guided by quality, transparency, and early involvement of all relevant stakeholders. Certification schemes should be designed to be neutral, allowing different technical solutions that achieve the same security objectives.

In this context, Article 72 should provide greater legal certainty by explicitly enumerating the categories of stakeholders represented in the European Cybersecurity Certification Assembly, rather than relying on an open-ended reference to «relevant stakeholders». Such categories should include, inter alia, ICT product and service providers (including SMEs), user and demand-side organisations, conformity assessment and national accreditation bodies, European and international standardisation organisations, supervisory authorities, academia, and civil society. Furthermore, Article 32(6) should be strengthened to ensure balanced and high-quality technical input across the entire lifecycle of certification schemes, including their development, revision, and maintenance. ENISA ad hoc working groups should therefore reflect a balanced representation of supply- and demand-side actors, SMEs, conformity assessment bodies, and standardisation expertise.

Article 74: Transparency and traceability in the scheme drafting process

Certification processes should be based on transparency and traceability, as a transparent scheme drafting process helps to build trust in certification schemes and improve their overall quality. Approaches that ensure the development of certification schemes remains understandable and traceable for relevant stakeholders, with technical considerations clearly communicated, are therefore welcome. To further enhance predictability and enable meaningful stakeholder participation, ENISA should be required to publish and regularly update an action plan for the development and maintenance of certification schemes, including key milestones and public consultation timelines. In addition, ENISA and the Commission should publish summaries of stakeholder feedback received during feasibility studies, scheme development and maintenance, together with explanations of how such input informed subsequent revisions.

Articles 75-76: Maintenance and evolution of certification schemes

Bitkom welcomes the introduction of a clear maintenance and review mechanism in Articles 75 and 76. To ensure the long-term effectiveness of certification schemes, it is

important that they are regularly reviewed and updated. The ongoing evolution of certification schemes should continue to involve all relevant stakeholders, ensuring that schemes remain up to date and aligned with evolving cybersecurity requirements. Technical specifications underpinning certification schemes should, as a general rule, be publicly available in order to ensure transparency, legal certainty, and equal market access.

In light of rapid technological developments, including advances in quantum computing, certification schemes and their technical specifications should also be designed to support crypto agility and post-quantum readiness. Regular updates should not only address newly identified vulnerabilities but also proactively mitigate foreseeable structural risks, thereby ensuring that certified products and services remain secure by design throughout their lifecycle.

Article 78: Presumption of conformity as a tool to support regulatory compliance

Bitkom supports the approach of using certification as an optional tool to facilitate regulatory compliance. Companies should have certainty that, if they choose to certify their overall cyber posture, products, services or processes to demonstrate under a European scheme, this will be sufficient to demonstrate compliance with EU legal requirements, without the possibility for Member States to ask for additional technical evidence. At the same time, it is important that certification schemes retain their voluntary nature and serve as a supportive mechanism for achieving regulatory objectives. Certification should help simplify compliance while preserving innovation and technological openness.

To ensure that certification effectively supports these objectives and delivers tangible security improvements, the CSA 2 should place greater emphasis on the independence, quality and continuous oversight of conformity assessment bodies. In particular, clear rules on the segregation of advisory and assurance functions are necessary to prevent conflicts of interest and maintain trust in certification outcomes. In this context, ENISA could take on a stronger coordinating role in promoting consistent accreditation and supervision practices across Member States, while respecting the operational independence of certification bodies.

Article 80: Security objectives of European cybersecurity certification schemes

The more than 20 objectives listed in Art. 80 represent a random collection of requirements that mix product obligations (cf. CRA Annex I), duties for service providers, and expectations for development processes. In contrast to the CRA, whose objectives in Annex I Part I (2) are explicitly risk based, Art. 80 formulates its objectives in absolute terms, without considering proportionality or risk. In addition, many of the objectives duplicate existing requirements from other regulations such as the CRA, NIS-2 and in parts also with AI Act and Machinery Regulation, which creates unnecessary overlap and potential inconsistencies. To avoid this fragmentation, the individual

objectives in Art. 80 should be removed. Instead, the regulation should reference the established objectives already defined in the relevant regulations, in particular the CRA and NIS-2.

In parallel, the certification system must be designed efficiently: ICT products, ICT services, and ICT processes or managed security services that have already been certified under existing schemes should be recognised across all Member States as valid evidence of conformity, as proposed in CSA-2, in order to avoid duplication and ensure practical coherence in implementation.

Article 81: Elements of European cybersecurity certification schemes

According to Article 81(3) (c), Member States may propose extension profiles introducing additional requirements for specific product categories. However, such extensions are only viable if they are uniformly adopted across all Member States and apply to the certification scheme as a whole. Allowing divergent national extensions would undermine the objective of harmonisation, create fragmentation within the internal market, and impose significant additional administrative and compliance burdens on companies. To safeguard legal certainty and ensure the effectiveness of the certification framework, extension profiles must therefore be applied consistently at EU level. Extension profiles should be limited to narrowly defined technical gaps and must not serve as a vehicle for introducing sovereignty-driven or other non-technical requirements at national level.

What is missing in Article 81, is an obligation on ENISA to ensure that all schemes under the ECCF include a mechanism that enables ‘continuous conformity’ without constant recertification. Unfortunately, the term only appears in Recital (93). Article 81(2)(a) contains some approaches but does not go far enough. At higher assurance levels, verification of compliance with technical documentation should remain proportionate and risk-based and should not be interpreted as requiring exhaustive validation of all documented security functionalities, particularly in the case of complex or continuously updated systems. Unfortunately, the only certification scheme that exists (EUCC) suffers from the recertification requirement: software with the certificate would usually be outdated and have known security vulnerabilities. So, you either use a current, secure version without a certificate, or an outdated, insecure version with a certificate. CSA-2 therefore needs to move significantly further away from a (tangible) product-based approach with a few exceptions.

4 TITLE IV: SECURITY OF ICT SUPPLY CHAINS

Secure, trusted and reliable ICT supply chains are crucial for the proper functioning of critical infrastructure as well as for the general society. Bitkom therefore supports the objectives pursued under Title IV to strengthen Europe's resilience against external shocks. Stronger EU ICT supply chains can make a meaningful contribution to European resilience, in particular where EU intervention supports harmonization across Member States, while respecting their competence to make decisions on national security matters.

Before introducing the ICT supply chain framework, the European co-legislators should also ensure that existing legislation is implemented and enforced more effectively, alongside considering whether additional regulatory measures are needed. Regulatory requirements can only achieve their intended objectives if consistently enforced. Existing enforcement deficits should be adequately addressed before any additional regulatory obligations are introduced. This is particularly important where existing rules, including the GDPR, the 5G toolbox or UNECE R155, already provide mechanisms to address risks such as unauthorised data access or data extraction within ICT supply chains.

In this regard, EU-level coordinated risk assessments can help reduce fragmentation and create more consistent security outcomes. At the same time, EU measures must fully respect decisions taken by Member States in relation to their national security, as harmonisation can only be effective where it complements rather than contradicts such decisions. To preserve these benefits, Member States should equally refrain from adding gold-plating to CSA-2, which would undermine a common EU-wide approach. . Given the sensitive balance between EU-level harmonisation and Member State responsibility for national security, it is essential that any measures remain clearly within the EU's competences under Article 4 Treaty of the European Union (TEU).

Legal certainty is also required regarding the activities that bring undertakings within the scope of Title IV. In particular, the framework should avoid capturing large industrial groups solely because they carry out ancillary, supportive or purely internal activities that may fall within a NIS-2 sector but are not system-relevant from a cybersecurity perspective. CSA-2 should therefore be clearly limited to the core business activities, ancillary activities that do not affect the resilience of essential or important services should not trigger additional obligations. This clarification would avoid an over-extension of the regulatory scope, reduce unnecessary administrative burden, and support the EU's simplification agenda, including the Omnibus and Digital Fitness Check initiatives. It would also help preserve a level playing field across the Single Market. While some Member States have already started to reflect a core-activity approach in their national NIS-2 transposition, divergent national interpretations may emerge in the absence of a clear EU-level legal basis. The core-activity principle should therefore be anchored directly at EU level to ensure harmonised application and legal certainty.

These scope-related concerns reinforce the need for a clear and robust legislative process. It is questionable whether an Implementing Act is the appropriate instrument for measures with such far-reaching implications and clear sector-specific impact. In line with Article 118, any particularly intrusive interventions within the envisaged framework should be subject to appropriate legislative scrutiny and meaningful involvement by the Member States. The European Commission should therefore not be empowered to take far-reaching decisions unilaterally where there is no qualified majority among Member States. At the same time, the framework should ensure that the decision-making process remains timely and effective, in particular where urgent security risks need to be addressed. Legal certainty regarding both the scope of application and the intensity of the obligations is indispensable.

The framework should also reflect that different categories of non-technical risk require different regulatory responses. While risks linked to undue influence by third countries may justify swift restrictive measures where substantiated, other risks — such as supplier dependency, market concentration or broader structural resilience concerns — require a more consultative, evidence-based and proportionate approach. Where suppliers are associated with a third country posing cybersecurity concerns, the framework should therefore provide for a structured consultation mechanism prior to the imposition of restrictive mitigation measures or high-risk designations. This would strengthen legal certainty, reduce the risk of unintended market distortions, and support a more coherent Single Market approach.

A robust legal framework alone, however, will not be sufficient. To be effective in practice, Title IV must also be supported by operational instruments that translate risk assessments into verifiable and consistently applicable security baselines across the Single Market. With CSA-2, the EU is moving to reinforce ENISA's coordination role including industry stakeholder engagement and to further develop the ECCF. This is important so that certification schemes such as EUCC, as well as ongoing work on schemes like EU5G and EUCS, can provide verifiable security baselines, enhance legal certainty and support consistent implementation across the Single Market. Title IV should take these baselines into account where possible, so that supply-chain measures remain coherent, implementable, and aligned with existing EU-level security mechanisms.

Even where such alignment is achieved, measures under Title IV must remain proportionate in their practical effects and must avoid creating unnecessary disruption for affected sectors. Where more restrictive measures are mandated for reasons of public interest, the resulting costs should not be shifted to affected entities and customers without adequate safeguards. The resulting costs must be financially compensated by the European Commission to safeguard competitiveness and prevent disruption.

Ensuring that the framework is legally sound, operationally workable, and economically proportionate will require close and continuous cooperation with relevant stakeholders across all affected industries. Structured stakeholder involvement is therefore essential not only to improve the quality and feasibility of the framework, but also to strengthen legal certainty, support consistent application across the Single Market and avoid unintended negative effects on innovation, investment, and resilience. Against this background, the following sections set out

detailed suggestions for the individual Articles of Title IV, with the aim of ensuring that the framework remains risk-based and proportionate.

Article 99: Security risk assessments

The regulation must mandate early industry engagement during the assessment phase to verify technical data, risks etc. Furthermore, the text must include a mechanism for judicial or administrative review of the risk assessment itself, allowing stakeholders to challenge findings before they trigger downstream designations.

The current drafting allows for the identification of "key ICT assets" and "threat scenarios" without mandatory consultation. Industry input is essential to ensure these foundational assessments rely on verifiable technical information. Since these assessments act as the irrevocable trigger for subsequent country and supplier designations, a review mechanism is necessary to strengthen procedural balance. It ensures that if factors considered are not proportionate or necessary, there is a legal avenue to prevent irreversible market distortions.

Further clarification is needed regarding the respective roles and scope of security risk assessments conducted by the European Commission and by the NIS Cooperation Group. While the latter is clearly limited to critical ICT services, systems, products, and supply chains, such a limitation is not evident for Commission-led assessments under Article 99. Clarifying why two distinct mechanisms are necessary, and whether Commission assessments are intended to extend beyond critical ICT assets, would significantly enhance legal certainty, predictability, and consistent implementation.

Article 100: Designation of third countries posing cybersecurity concerns

Article 100 should provide for a clarified process regarding designation of third countries as posing cybersecurity risks. It should also clarify when such designation triggers subsequent steps under the framework that may lead to designations and exclusions to ensure consistency and predictability across the internal market, while safeguarding proportionality as laid down in recital 144 and related provisions in Articles 102-104. A more coherent approach would rely on horizontal country assessments at the EU level, as defined in article 100. These assessments could be informed by targeted sector-specific risk assessments under article 99 and subsequent articles 101-104, leading to the identification and application of measures.

The procedural framework should also be further specified: while coordinated risk assessments by the NIS Cooperation Group are subject to defined timelines, comparable safeguards are lacking for Commission-led assessments under Article 100. The regulation should therefore introduce clear time limits and more precise rules on the scope and interaction of these procedures in order to prevent parallel or open-ended assessments, reduce fragmentation, streamline procedures, and avoid prolonged uncertainty for affected entities, suppliers, and supervisory authorities that could delay investment and compliance decisions.

Furthermore, the application of Article 100 must reflect the inherent limitations of cybersecurity risk attribution and enforcement. As a result, risk designations under Article 100(1)(d) should be applied with particular caution. The CSA 2 framework contains proportionality safeguards, in particular in Recitals 144 and 145 and Articles 102–104. These safeguards should remain central to the application of Article 100, ensuring that third-country designations are not used excessively or as a precaution, while allowing for a comprehensive and case-by-case assessment of relevant risk factors.

In applying Article 100, particular care should be taken to avoid unintended consequences for globally active companies that, while headquartered outside the Union, are deeply integrated into European value chains. A proportionate approach should ensure that participation in EU certification, standardisation and advisory processes is restricted only where clearly substantiated security risks have been identified.

Article 102: Identification of key ICT assets

The scope and methodology for identifying «key ICT assets» should be transparent, risk-based and linked to concrete operational scenarios. Where appropriate, the process may benefit from consultation mechanisms of industry experts to ensure technical robustness, while preserving the ability of competent authorities to act in a timely and proportionate manner.

Where the criteria refer to vulnerabilities being «known to have been exploited», the Regulation should clarify that «exploitation» means malicious exploitation. Without such a clarification, proof-of-concept activity commonly used by security researchers to verify vulnerabilities could be misinterpreted as «active exploitation». This would undermine responsible vulnerability research and disclosure practices and could discourage security testing that contributes to the overall resilience of ICT products and services. Aligning this terminology with established approaches in EU cybersecurity legislation would avoid unintended consequences and strengthen the credibility of the risk assessment framework.

Article 103: Mitigation measures in the ICT supply chain

Mitigation measures under Article 103 should be risk-based, proportionate, and operationally feasible, avoiding a one-size-fits-all approach. Given the far-reaching implications and clear sector-specific impact of such measures, any particularly intrusive interventions should be subject to appropriate legislative scrutiny rather than being introduced solely by means of an implementing act. Before the Commission takes any measures under Article 103(1), stakeholders and industry should be consulted to clarify the underlying concerns and to provide input on satisfactory mitigation measures. To strengthen legal certainty and ensure a consistent risk-based application, Bitkom urges the co-legislators to amend Article 103 so that measures are strictly aligned with the risk scenarios developed under Article 99(1). In particular, high-impact measures such as prohibitions should be limited to high-risk scenarios where

systemic disruption is likely, while low-risk scenarios should be addressed through less intrusive and more targeted measures.

The framework should include grandfathering provisions for deployed systems and components and should avoid mandatory replacement or retrofitting of existing products, given the significant lead times and efforts typically involved. This is particularly relevant for already deployed and complex products, where retrofitting may require entirely new supply chains, substantial re-engineering, additional production capacity, and costly recall procedures, often over several years and at costs amounting to billions of euros. Where measures affect future procurement or new deployments, sufficiently long and predictable transition periods are necessary to enable orderly adaptation, alternative sourcing, and, where required, redesign of affected components. Article 103 should therefore clearly distinguish between measures applicable to new deployments and those affecting existing systems, ensuring that obligations remain forward-looking and aligned with realistic industry timeframes and development cycles.

In addition, greater clarity is needed on the scope and downstream effects of high-risk supplier designations. It must be specified whether restrictions apply to all products supplied by a designated company or only to specific components, and how such designations would affect manufacturers placing products with digital elements on the market where those products rely on components from the designated supplier. Any resulting obligations must remain proportionate to the criticality and operational exposure of the affected systems.

Article 100(4): Consequences of designation

We propose adding a new paragraph to Article 100 establishing a formal European Commission procedure through which suppliers can respond to and contest a high-risk designation, while ensuring that the process remains clearly time-bound and reaches a definitive conclusion. This should createa direct link with the exemption mechanism in Article 105(2). Article 100(4) currently prohibits designated suppliers from holding European cybersecurity certificates, which acts as a disproportionate market barrier. Under the CRA, these certificates are critical for demonstrating conformity without the costly and time-consuming involvement of a Notified Body. Current alternatives, such as informal "Enhanced Scrutiny" or mandatory bespoke EU schemes, either lack practical enforceability or diverge significantly from established global standards. A formalized procedure based on cumulative compliance with international standards and EU law would address this by ensuring that suppliers have a meaningful opportunity to be heard, while preserving rigorous security standards and preventing rigid, anti-competitive market lockouts.

Article 104: Identification of high-risk suppliers

Any assessment and decision on restrictive measures should be grounded in clearly defined risk scenarios and must take into account the operator’s and the countries overall security concept as laid down in recitals 144, 145 and corresponding considerations laid down in articles 103 and 104. In particular, and in line with the

proposal this assessment should reflect the finding in coordinated Union risk assessments of key ICT criticality of the asset concerned, its operational exposure, and the effectiveness of existing technical and organisational safeguards. Criteria related to ownership or control should be considered, where they are proportionate, demonstrably relevant to the specific risk.

Terms such as «establishment» or «control» require precise and narrow interpretation. «Establishment» should be limited to the jurisdiction of legal incorporation and the location of ultimate effective corporate control, rather than mere operational presence. Likewise, any criterion relating to control by a third country should be based on legally enforceable control, taking into account the specific characteristics of the third country's legal system, in order to avoid. Governance-related factors may be relevant where suppliers are subject to third-country legal frameworks that can require cooperation with state authorities without sufficient transparency, judicial oversight or effective legal remedies, or where companies are directly or indirectly state-owned or subject to significant state influence. Such factors can raise legitimate concerns regarding data access, supply chain integrity, vulnerability management and long-term operational independence. Where relevant, they should therefore be assessed as part of a broader risk analysis, alongside technical security capabilities and feasible mitigation measures. Any reliance on ownership- or control-related criteria must remain proportionate, be grounded in demonstrable risk, and avoid abstract or purely formal classifications that are not tied to concrete cybersecurity outcomes.

To ensure that any identification methodology is effective and workable in practice, the European Commission should systematically consult not only competent authorities and member states, but also representatives of entities within the scope of the regulation. This is essential to make use of industry expertise, including on the availability of alternative sources and realistic mitigation options.

Any EU-level approach should complement as CSA ICT framework aims to, rather than override or conflict with, established national frameworks and competences. The Commission should ensure a high degree of predictability for affected companies, reflect typical business and procurement processes, and provide sufficient transposition and implementation periods through early engagement with stakeholders, including Member States and representatives from affected industries. Only a proportionate, asset-based and practically implementable framework will strengthen cybersecurity without undermining operational resilience and investment planning.

Article 105: Exemption for entities established in or controlled by entities from a third country posing cybersecurity concerns

It is good that Article 105 ensures market access and enables entities from a third country posing cybersecurity concerns designated in accordance with Article 100 can ask for an exemption from the prohibition. The proposed ICT supply chain security framework inevitably generates additional administrative burden for companies demonstrating supply chain compliance. To preserve the competitiveness of EU

businesses, any such burden must be strictly minimized and proportionate to the intended security objective. Currently, while Article 105(5) states the Commission "shall" grant an exemption, Article 105(4)(c) renders this conditional, introducing unpredictability into the "Union's interest" assessment. To create necessary legal certainty, the framework must clarify how "effective mitigating measures" under Article 105(2)(b) are evaluated.

Article 115: Penalties

The proposed penalties of up to 7% of worldwide net sales should be significantly reduced. The obligations in question affect society as a whole and extend beyond the core interests, influence, and control of private companies. Penalties should therefore remain proportionate and be capped at a maximum of 2% of total net sales.

Chapter II: ICT supply chains in electronic communications networks

The Commission’s proposal in Chapter II of Title IV to exclude ICT components, or components that include ICT components, from mobile, fixed and satellite electronic communications networks would impose serious practical and economic burdens on network operators and undermine Europe’s connectivity objectives. This approach would extend far beyond the scope of the EU 5G Toolbox, especially with regard to fixed and satellite networks. It would entail substantial financial burdens and significant organisational challenges. The proposal should therefore be anchored more clearly in differentiated risk scenarios and tailored to the level of criticality and exposure of the relevant network functions, rather than applying broadly across heterogeneous network types.

This need for a differentiated approach is also essential from a procedural perspective. The CSA-2 proposal introduces sector-specific measures that apply elements of an ICT supply chain security framework before that framework itself has been adopted. As a result, it risks imposing broad restrictions on the telecommunication sector without first establishing the common criteria, safeguards and procedures needed to assess ICT supply chain risks consistently across all sectors in scope. The appropriate sequence should be to first establish the legal framework for ICT supply chain security and then apply the agreed process consistently, based on the criticality and exposure of the relevant functions, rather than introducing sector-specific exclusions in advance.

This sequencing concern is not merely formal. Introducing broad sector-specific exclusions without a fully established risk-assessment framework would have direct consequences for network planning and investment. The proposed broad exclusion requirements come at a time when Europe must accelerate the rollout and upgrade of resilient connectivity infrastructures. Network operators would face conflicting priorities and have to divert capital away from network improvements and expansion. In an environment of growing geopolitical tensions, the framework must support the enforcement of security measures in relation to the risks posed by threat actors. At the same time, it must ensure that risk mitigation does not undermine operational capability or the ability to expand and modernise networks at the necessary speed.

The cost assumptions underpinning the proposal require greater transparency and realism. Current estimates indicate that expansion and replacement costs across European mobile, fixed and satellite infrastructures would amount to several billions of euros. They should therefore be assessed on a robust and comparable basis and reflected accordingly in the policy design. Where public-interest objectives lead to mandated replacements, compensation mechanisms should be established in line with the approach set out above.

For these reasons, Bitkom considers that Articles 110 and 111 should be fundamentally questioned. At a minimum, any retained measures must be proportionate and subject to clear safeguards, specifically they should: be grounded in a robust economic impact assessment; not contradicting existing national security decisions taken at Member State level; take due account of established de-risking approaches; fully explore and consider less intrusive mitigation measures.

Bitkom represents more than 2,300 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 700 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact person
Felix Kuhlenkamp | Head of Security
P +49 30 27576-279 | f.kuhlenkamp@bitkom.org

Responsible Bitkom Committee
WG Security Policy

Copyright
Bitkom 2026

This publication is intended to provide general, non-binding information. The contents reflect the view within Bitkom at the time of publication. Although the information has been prepared with the utmost care, no claims can be made as to its factual accuracy, completeness and/or currency; in particular, this publication cannot take the specific circumstances of individual cases into account. Utilising this information is therefore sole responsibility of the reader. Any liability is excluded. All rights, including the reproduction of extracts, are held by Bitkom.