EUROSMART
The Voice of the Digital Security Industry

Response to the Public Consultation on the Revision of the EU Cybersecurity Act (CSA2)

1. CSA2: Unlocking the Full Potential of EU Cybersecurity Certification

1.1. Strengthening and Scaling the European Cybersecurity Certification Framework

Eurosmart welcomes the European Commission's initiative to revise the Cybersecurity Act (CSA2). This revision comes at a critical moment, as Europe faces an increasingly complex cybersecurity landscape shaped by rapid technological evolution and growing threat sophistication.

The original Cybersecurity Act laid the foundations for a European cybersecurity certification framework. However, this framework now requires a fresh impetus to fully deliver on its objectives. To date, the EUCC scheme remains the only operational European cybersecurity certification scheme, while additional schemes are urgently needed to support the broader EU digital regulatory landscape. The development of new certification schemes will be essential to underpin key EU policy initiatives and regulatory frameworks that rely on EU cybersecurity certification schemes, especially in areas such as cloud services, the EUDI Wallet, AI, 5G, and IoT, PQC, edge computing, IIOT, automotive...

In this context, both the development of new schemes and their effective maintenance should be further supported as key enablers of the EU cybersecurity ecosystem, ensuring that the certification framework can keep pace with technological and regulatory developments.

CSA2 also introduces mechanisms addressing non-technical cybersecurity risks. While these respond to legitimate concerns, Eurosmart considers that such factors are not yet fully framed within a clear and coherent approach. By nature, these mechanisms relate to structural and geopolitical risk considerations, rather than to technical cybersecurity assessment.

CSA2 therefore represents a necessary and timely evolution to ensure that the framework becomes more dynamic, scalable, and responsive to operational realities, while supporting the Union's broader strategic objectives.

Eurosmart supports the ambition to strengthen certification governance and improve international recognition mechanisms.

At the same time, targeted refinements are necessary to ensure that the revised framework preserves its technical credibility, provides legal certainty and predictability, and avoids unintended spillovers between technical certification and broader geopolitical considerations.

1.2. Need for a Security-driven Scheme Roadmap

The proposal no longer maintains the former Union Rolling Work Programme, therefore a security-driven and risk-based approach to the prioritisation of European cybersecurity certification schemes is needed to ensure that Union efforts and resources focus on technologies and use cases presenting the highest cybersecurity, resilience and strategic dependency risks.

A security-driven certification roadmap is needed. To maximise impact, scheme prioritisation should be anchored in risk and criticality, including security-critical hardware components, scalable IoT/embedded assurance, cryptographic components supporting PQC/crypto-agility, digital identity/trust services, and cloud/edge components. This would guide resources towards the areas where EU certification can most effectively raise assurance and reduce fragmentation.

1.3. Industry-Driven Scheme Development and Mandatory Market Assessment

Industry stakeholders should be able to propose candidate European cybersecurity certification schemes or priorities for future scheme development, in particular where emerging technologies, sector-specific needs or significant cybersecurity risks are identified. Since the objective of European cybersecurity certification schemes is notably to support the development, uptake and trustworthiness of secure ICT products, ICT services and ICT processes within the Union market, Eurosmart supports the establishment of structured consultation and request mechanisms enabling industry, competent authorities and relevant stakeholders to contribute to the identification of certification priorities.

In order to ensure transparency, proportionality and evidence-based prioritisation, the preparation or update of certification schemes should be supported by mandatory market and impact assessments, including stakeholder surveys, covering market needs, cybersecurity relevance, technological maturity, existing standards, implementation feasibility and potential impact on industry and SMEs.

Moreover, Eurosmart further welcomes Article 75(4)(c), which enables consultation of relevant stakeholders in the process of updating European cybersecurity certification schemes, and stands ready to actively contribute to such consultation processes in support of effective, operational and market-relevant certification frameworks.

1.4. Transition from National Schemes to EU schemes

The transition from national cybersecurity certification schemes to European schemes must be carefully managed to preserve legal certainty, operational continuity and market stability. Previous transitions have shown that insufficient migration safeguards may create unnecessary costs and delays for manufacturers without corresponding security benefits. Future transitions should therefore ensure appropriate transition periods, continuity of existing certificates and the possibility to reuse existing evaluation evidence where appropriate.

2. Strengthening the Governance and Maintenance of Certification Schemes

2.1. Maintenance Strategy as a Core Pillar of Certification Credibility

Eurosmart underlines that the credibility and effectiveness of European cybersecurity certification schemes depend fundamentally on their ability to be continuously maintained and updated, supported by a clear and structured maintenance strategy.

Cybersecurity certification is not static: it must evolve in line with emerging threats, technological developments, and operational feedback from implementation. In this context, effective maintenance should also include the identification and mobilisation of relevant stakeholders capable of supporting certification schemes, ensuring that the necessary expertise is consistently available throughout the lifecycle of the scheme.

Eurosmart therefore welcomes **the introduction of the maintenance strategy** as defined in Article 75(3). This strategy should be embedded in certification schemes from their creation and accompany them throughout their lifecycle. Doing so ensures clarity, predictability, and continuity in how schemes evolve over time, while enabling structured stakeholder involvement.

Without such a robust and forward-looking maintenance framework, certification schemes risk becoming outdated, undermining both their security value and their market relevance.

2.2. A More Agile Maintenance Model through Technical Specifications

Eurosmart strongly supports the reinforced role of ENISA and the introduction of a more agile maintenance model based on technical specifications.

This approach represents a clear improvement compared to the current reliance on implementing acts, enabling faster and more responsive updates to certification schemes in line with evolving threats and technologies.

Eurosmart also welcomes the provision that technical specifications shall be published on ENISA's website, **except where security concerns justify restricted access**. This balanced approach is essential to ensure both transparency and the protection of sensitive information.

This is particularly important for schemes such as EUCC, where certain maintenance elements, such as attack catalogues, contain highly sensitive information (e.g. attack methods) that must remain appropriately protected.

Overall, this model provides the necessary flexibility to maintain schemes at the state of the art while preserving the stability of the regulatory framework.

2.3. Structured Stakeholder Involvement as a Key Enabler

Eurosmart emphasises that cybersecurity expertise is widely distributed across industry, certification bodies, national authorities, and sectoral communities.

As recognised in Recital 90, the contribution of stakeholders - including ISACs and standardisation organisations - is essential to ensuring that certification schemes remain aligned with real-world needs and technological developments.

Structured stakeholder involvement should therefore be considered a **core component of maintenance governance**, rather than a secondary or optional element. Without it, schemes risk losing both technical relevance and industry support.

Expert participation should be based on competence. While balanced participation is important, the effectiveness and security relevance of schemes depends on experts being selected primarily on demonstrated technical competence and domain experience. Inclusiveness objectives should not unintentionally deter highly qualified experts or create ambiguity about selection criteria.

2.4. Role of ISACs and Maintenance Governance

Eurosmart considers that Article 75 should be clarified and strengthened to ensure that stakeholder involvement is explicitly recognised and effectively implemented in practice, and that it fully reflects the intentions set out in Recital 90.

ENISA should regularly work with relevant stakeholders, including ISACs, and make stakeholder engagement a key part of its maintenance activities. ENISA should be able to organise structured engagement mechanisms, such as sectoral liaison arrangements, and, where appropriate, ad hoc working groups.

ENISA ad hoc working groups should remain an available option, in particular in cases where relevant stakeholder interaction cannot be clearly identified or where no established stakeholder ecosystem exists.

At the same time, Eurosmart stresses the importance of building on existing and well-functioning stakeholder ecosystems. Relying on already established stakeholder groups would ensure continuity of expertise and better alignment with real-world deployment realities. Structures such as the EUCC ISAC already provide consolidated expertise and established cooperation frameworks and should therefore be preserved and actively leveraged.

Any new mechanisms should complement these existing structures, rather than duplicating or bypassing them.

2.5. Transparency, Consultation and Effectiveness of the Maintenance Framework and Schemes' development

Eurosmart underlines that transparency and inclusiveness are essential to the effectiveness of the functioning of the European Cybersecurity Certification Framework.

Where ENISA relies on ad hoc working groups for maintenance activities or for the development of certification schemes, intermediary consultation steps should be systematically foreseen. This is necessary to ensure that broader stakeholder expertise is taken into account and to avoid overly closed or opaque processes.

Eurosmart emphasises that maintenance schedules and technical updates should be predictable and based on technical feasibility, reflecting industry cycles to ensure trust and effectiveness in European cybersecurity certification schemes.

A maintenance framework combining agility, structured stakeholder involvement, and transparency will significantly enhance the quality, credibility, and usability of certification schemes, while supporting their long-term uptake across the market.

2.6. Predictability and operational transparency are prerequisites for uptake

Eurosmart supports the introduction of fee mechanisms to ensure sustainable scheme operation. However, fees should remain transparent, proportionate and linked to clearly defined maintenance and support deliverables, with indicative timelines to preserve predictability for market operators and avoid discouraging uptake, notably for SMEs.

In parallel, transparency should go beyond access to documents and provide lifecycle visibility on scheme evolution (maintenance activities, technical specifications, transition rules) and traceability of stakeholder input, while preserving confidentiality and security-sensitive information.

This should be reflected in articles 47 & 53.

2.7. Scheme withdrawal

Scheme withdrawal must remain exceptional and include transition safeguards. Withdrawal of a European scheme can disrupt markets and long-lifecycle investment decisions. Any withdrawal should therefore follow a thorough impact assessment and provide sufficient transition periods, including continued validity of existing certificates for their full duration and clarity on alternative certification paths, to avoid undue disruption and preserve legal certainty. This should be reflected in article 76.

2.8. Oversight proportionality

Oversight mechanisms should remain exceptional and proportionate. Conformity assessment bodies are core to the framework; additional EU-level measures should not create a “fourth layer” of supervision. Where applied, measures should be duly reasoned, proportionate, and without prejudice to the primary role of national accreditation and certification authorities, taking into account impacts on ongoing certifications and market continuity.

Article 94 should reflect this, maintaining its role as an exceptional corrective measure instead of becoming a lasting parallel EU supervisory system for conformity assessment bodies.

2.9. Role of the ECCG and Member States in CSA2 Governance

Eurosmart considers that the European Cybersecurity Certification Group (ECCG) and Member States should retain a central role throughout the governance, preparation, maintenance, supervision and international dimension of the European cybersecurity certification framework.

Given the operational and strategic importance of European cybersecurity certification schemes, Eurosmart underlines the need to preserve an appropriate institutional balance between the Commission, ENISA, the ECCG and national cybersecurity certification authorities. In particular, the ECCG and Member States should remain closely involved in:

- the identification and prioritisation of candidate certification schemes;

- the preparation, review and maintenance of European cybersecurity certification schemes;
- the development and review of technical specifications and maintenance activities;
- peer review and oversight mechanisms, notably for assurance level "high";
- ICT supply-chain risk assessments and qualification mechanisms under Title IV;
- and international recognition and equivalence decisions.

3. Preserving the Technical Credibility and Integrity of the "High" Assurance Level

3.1. Mandatory Penetration Testing and Evidence-Based Evaluation Against Advanced Attacks

Eurosmart considers that the credibility of European cybersecurity certification depends critically on the robustness and consistency of assurance levels, particularly the "High" assurance level.

In this context, **penetration testing[1] must remain a mandatory requirement for ICT products, ICT services, ICT process, Manages Security Services and cyber posture of entities** at this level.

Penetration testing is the only rigorous and operationally relevant method to assess the resistance to skilled and adaptive attackers. Introducing discretion through wording such as "where relevant" risks weakening the assurance level, creating inconsistencies across schemes, and reducing trust among users, particularly in critical sectors.

While some flexibility may be justified for ICT services and ICT processes, such flexibility is not appropriate for ICT products and security-critical components, which must demonstrate resilience against realistic attack scenarios linked to realistic attacker capabilities, including advanced logical, side-channel and physical attacks where relevant for security-critical products and components.

Eurosmart also underlines that "High" assurance must remain evidence-based. Security objectives and evaluation methodologies should therefore be explicitly linked to measurable and technically verifiable evidence and to realistic attacker capabilities, including advanced logical, side-channel and physical attacks where relevant for security-critical products and components, while avoiding overly declarative or process-only approaches. Certification schemes should ensure that evaluation methods appropriately reflect realistic attacker capabilities in order to preserve trust and technical credibility across European cybersecurity certification schemes.

Maintaining mandatory penetration testing and robust technical evaluation requirements is therefore essential to ensure a consistent level of cybersecurity assurance, strengthen trust

[1] *"Penetration testing is the act of locating weaknesses and vulnerabilities of devices and information systems by anticipating the intent, actions and skills of malicious hackers. Ethical Hacking is done on a defensive purpose with the objective to improve the security of devices and information systems, and to give assurance that they will resist to attacks with similar intent, actions and skills once released and operated."*
Eurosmart, Cybersecurity Act: Ethical hacking does matter! 1 June 2018

in EU certification schemes and support their global recognition. This should notably be reflected in Articles 80, 81 and 82.

3.2. Peer Review and Technical Expertise under Assurance Level "High"

Eurosmart notes that Regulation (EU) 2019/881 explicitly provided, under the peer assessment mechanism, for the assessment of whether authorities or bodies issuing certificates at assurance level "high" possessed the appropriate technical expertise. While the CSA2 proposal maintains peer review mechanisms and assurance level "high", this explicit reference no longer appears to be retained in Article 89.

This is particularly important given that certification activities at assurance level "high" increasingly rely on advanced technical evaluations, including vulnerability analysis and penetration testing, requiring highly skilled personnel and sufficient operational expertise. Eurosmart therefore considers that **Article 89 should explicitly provide that peer review mechanisms include assessment of the technical expertise, capabilities and appropriate resources of authorities and bodies involved in high-assurance certification activities**, in order to preserve trust, consistency and credibility across the Union.

In addition, removing this provision from the CSA2 will create two types of certificates of assurance level "high". Those issued under Regulation (EU) 2019/881 for which the technical expertise, capabilities and appropriate mechanisms of National Cybersecurity Certification Authorities is verified through the peer review, and those issued under the CSA2 for which these aspects have not been ascertained through peer review. This will be a substantial downgrade of trustone could place in a certificate of assurance level "high".

4. Cryptographic Aspects under CSA2

4.1. Cryptographic Transition under CSA2 - PQC Roadmap, Standardisation and Certification Alignment

Eurosmart highlights the strategic importance of properly addressing the transition towards post-quantum cryptography (PQC) within the European cybersecurity certification framework. While quantum threats are evolving, this transition must be carefully prioritised and designed to ensure effective and timely adoption by industry and stakeholders.

Eurosmart underlines that PQC deployment should be driven by a clear and accelerated roadmap, based on well-identified use cases, sectors, and ICT products and/or ICT services, with a particular focus on critical sectors and long-lifecycle systems where early migration is necessary. A structured and implementable migration approach, as outlined in Commission Recommendation (EU) 2024/1101, is essential and should build on international best practices.

Eurosmart also stresses that the transition must consider the current state of standardisation and technological maturity. The absence of fully stabilised and widely adopted standards, despite ongoing initiatives such as those identified in the European Commission Annual Union Work Programme (AUWP) for 2026, remains a significant challenge and may hinder effective and coordinated deployment.

In this context, ENISA should play a central supporting role in:

- identifying priority use cases, sectors, and relevant ICT products and/or ICT services;
- assessing technical and operational gaps;
- contributing to the development of standards and technical specifications, including in the context of European cybersecurity certification schemes.

Finally, alignment with other EU frameworks should be ensured, including through possible targeted adjustments to Directive (EU) 2022/2555 (NIS2 Directive), notably in the context of simplification efforts and coherence with CSA 2.

4.2. Emerging Cryptographic Techniques Supporting Privacy - Need for Maturity, Standardisation and Certification Readiness

Eurosmart also highlights the growing importance of emerging cryptographic techniques supporting privacy, which are gaining traction, in particular in the context of the European Digital Identity Framework (EUDI Wallet) established by Regulation (EU) 2024/1183.

While these techniques offer significant potential to enhance privacy and data protection, they currently face key challenges:

- the lack of broad scientific and industrial consensus regarding their security robustness;
- the absence of mature, widely recognised standards, beyond vendor-specific implementations;
- limited interoperability and certification readiness.

These gaps may hinder their large-scale deployment and uptake within European cybersecurity certification schemes.

In this context, ENISA should play a pivotal role in:

- supporting the development of robust, interoperable standards;
- fostering consensus within the technical community;
- assessing their suitability for integration into certification frameworks;
- facilitating their progressive and secure adoption in high-impact use cases such as digital identity.

A cautious and structured approach is therefore necessary to ensure that the integration of such techniques into the European cybersecurity framework is secure, interoperable, and sustainable.

5. ENISA's Role and Supporting Missions under CSA2

Eurosmart supports a strong and operational role for European Union Agency for Cybersecurity in supporting the implementation of the Union cybersecurity framework. ENISA should continue to act as a centre of expertise, coordination and technical support, while preserving a clear distinction between advisory, coordination, certification and supervisory functions.

5.1. ENISA Support for CRA Manufacturers and Economic Operators

Eurosmart considers that ENISA's support role should also extend to manufacturers and economic operators subject to Regulation (EU) 2024/2847, notably through technical guidance supporting secure-by-design approaches, cybersecurity maturity and practical implementation of Union cybersecurity requirements.

In particular, ENISA could support:

- the dissemination of cybersecurity best practices,
- implementation guidance for SMEs and economic operators,
- the development of cybersecurity maturity approaches,
- and alignment between the Cyber Resilience Act, European cybersecurity certification schemes and other Union cybersecurity frameworks.

5.2. Technical Specifications, Standards and Role Separation

Eurosmart underlines that technical specifications must preserve a clear separation of roles and remain grounded in recognised standards and open processes. While agile updates and technical specifications may support responsiveness and operational adaptation, technical specifications influencing certification outcomes should rely on recognised European or international standards, or on transparent and inclusive multi-stakeholder processes.

ENISA's role should therefore remain focused on coordination, facilitation and technical support, without creating any de facto approval, supervisory or quasi-regulatory layer over certification applications, certification decisions or conformity assessment activities. Preserving a clear separation between technical support, certification governance and supervisory functions remains essential to ensure impartiality, predictability and trust in the European cybersecurity certification framework.

Eurosmart therefore considers that this principle should be reflected more clearly in Article 77.

6. International Recognition and Oversight of Third-Country Schemes (Article 87)

Eurosmart supports international cooperation and the recognition of third-country certification schemes, as this is key to avoiding market fragmentation and promoting European standards globally.

However, equivalence assessments must remain grounded in technical, objective and transparent criteria and should be supported by structured technical consultation and appropriate expert involvement.

The current framework raises concerns regarding the potential influence of political or commercial considerations. In addition, the absence of structured mechanisms to assess third-country supervisory, accreditation and conformity assessment frameworks create a gap compared to the internal EU framework.

Within the Union, peer review mechanisms, supervisory requirements and harmonised governance structures contribute to consistency and mutual trust. **No equivalent mechanism currently exists for third-country frameworks, creating asymmetry and potential risks for the integrity and credibility of European cybersecurity certification schemes.**

Eurosmart therefore supports strengthening the technical and governance dimension of equivalence assessments, including through expert consultation and appropriate review of third-country supervisory and conformity assessment frameworks. In this context, decisions relating to the recognition or equivalence of third-country certification schemes should be adopted through transparent and structured procedures, **including by means of implementing acts**, in order to ensure legal certainty, consistency, transparency and appropriate involvement of Member States and relevant technical expertise.

7. ICT Supply Chain Security and Non-Technical Risks (Title IV - Chapter 1)

Eurosmart welcomes the establishment of a Union-level framework to address risks related to ICT supply chains, including non-technical cybersecurity risks, as an important step in strengthening the resilience of the European cybersecurity ecosystem. However, the proposed framework raises several concerns

7.1 Consistency and Coordination with the NIS2 Framework

Eurosmart underlines the importance of ensuring consistency and appropriate coordination between the proposed ICT supply chain framework under Title IV and the governance and risk management mechanisms already established under Directive (EU) 2022/2555 (NIS2 Directive).

Several provisions of the proposed framework overlap with existing mechanisms established under the NIS2 Directive, notably Article 14 relating to the role of the NIS Cooperation Group, Article 21 relating to cybersecurity risk-management measures, including supply-chain security requirements, and Article 22 relating to coordinated security risk assessments of critical supply chains. Such overlaps are particularly relevant where ICT supply chain risk assessments concern sectors or entities falling within Annex I or Annex II to the NIS2 Directive.

In this context, appropriate articulation with the NIS Cooperation Group established pursuant to Article 14 of the NIS2 Directive should be ensured in order to preserve coherence with existing Union cybersecurity governance structures and avoid unnecessary duplication of mechanisms at Union level as well as inconsistencies.

Eurosmart considers that maintaining a clear distribution of responsibilities between Union-level coordination and Member State competences **is particularly important from a subsidiarity and proportionality perspective**. As the NIS2 framework already establishes sector-specific cooperation and coordinated cybersecurity risk-management obligations involving competent national authorities and Member States, the introduction of parallel governance or risk assessment mechanisms under CSA2 could create legal uncertainty, operational inconsistencies and unnecessary administrative complexity

Table 1. Mapping of Overlaps and Dependencies Between CSA2 and the NIS2 Framework

CSA2 Proposal Provision	Related NIS2 Provision	Nature of overlap / dependency	Comments
Article 99 - ICT Supply Chain Risk Assessment	Articles 14(4)(i) and 22	Coordinated ICT supply-chain risk assessments	Article 99 introduces Union-level ICT supply-chain risk assessment mechanisms which substantially overlap with the coordinated risk assessment framework already established under the NIS2 Directive. Appropriate coordination with the NIS Cooperation Group appears necessary to preserve consistency and avoid duplication.
Article 99(1), first, second and third sentences - ICT Supply Chain Risk Assessment	Article 22(1)	Coordinated security risk assessments and governance framework	Article 99(1) overlaps with Article 22(1) NIS2 by establishing rules governing the preparation, scope and content of coordinated ICT supply chain risk assessments. These provisions may effectively modify the governance and operational functioning of the NIS Cooperation Group established under NIS2, while extending the coordinated risk assessment framework beyond critical supply chains.
Article 99(2)	Article 22(1)	Timelines and procedural governance	Article 99(2) introduces procedural and timing requirements for coordinated ICT supply chain risk assessments, potentially affecting the functioning and governance framework of the NIS Cooperation Group.
Article 99(3)	Article 22(2)	Identification of ICT supply chain risks	Article 99(3) extends the scope of Article 22(2) NIS2 by empowering the Commission to identify additional ICT services, ICT systems or ICT products subject to ICT supply chain risk assessment mechanisms.
Article 99(3)(b)	Article 22(1)	Competence for conducting risk assessments	Article 99(3)(b) may create a contradiction with Article 22(1) NIS2 by granting the Commission powers to conduct ICT supply chain risk assessments, whereas Article 22 NIS2 relies on the NIS Cooperation Group framework.
Article 103 - Governance, Implementation and Review	Article 21	Cybersecurity risk-management obligations	Certain governance and implementation provisions may overlap with cybersecurity risk-management obligations already applicable to essential and important entities under the NIS2 Directive.

Article 103(2)(c) and Article 103(3)	Article 21(2)(a) and (e)	Technical and organisational cybersecurity measures	Some provisions relating to governance, consultation and operational measures may overlap with technical and organisational security measures already addressed under NIS2.
Article 113 - Cooperation Mechanisms	Article 14	Union-level cooperation and coordination	The cooperation mechanisms introduced under CSA2 may overlap with the role and activities of the NIS Cooperation Group established under the NIS2 Directive.
Article 114 - Supervision and Enforcement	Articles 31, 32 and 33	Supervisory and enforcement mechanisms	The supervisory framework applicable to entities covered by CSA2 may overlap with supervisory and enforcement mechanisms already established under NIS2 for essential and important entities.
Article 115 - Penalties	Article 34	Penalty framework	The introduction of additional penalty mechanisms may create overlap with existing NIS2 sanctioning regimes applicable to the same categories of entities.
Article 116 - Mutual Assistance	Article 37	Mutual assistance and cooperation mechanisms	CSA2 mutual assistance provisions may duplicate or overlap with existing cooperation and mutual assistance mechanisms under NIS2.
Article 117 - Jurisdiction and Territoriality	Article 26	Jurisdiction rules	The proposed jurisdictional framework may overlap with existing territoriality and jurisdiction rules established under NIS2.
Article 118(1) - Committee Procedure	Article 39	Committee governance	The committee structure introduced under CSA2 appears closely connected to existing governance mechanisms established under the NIS2 Directive.
Annex I - Certain Conformity Assessment Activities	Scope and sectoral framework of Directive (EU) 2022/2555	Applicability to conformity assessment bodies	Certain CSA2 provisions may indirectly impose cybersecurity-related obligations on conformity assessment bodies, although their relationship with the NIS2 framework remains unclear and may require clarification.

7.2. A Discretionary and Geopolitical Framework Beyond Technical Certification

At the same time, Eurosmart considers that the current approach would benefit from a clearer and more structured framework. The proposed mechanism addresses risks related to third-country systemic factors, supply chain dependencies, and broader strategic vulnerabilities. By their nature, they go beyond technical assessment and include policy judgement and strategic evaluation.

They are therefore discretionary and evaluative rather than purely technical, providing the Commission with a significant margin of discretion.

In this respect, Eurosmart underlines that this framework constitutes a **geopolitical risk management tool**, which must remain clearly distinct from the logic of technical certification and equivalence under Article 87.

Finally, while formally based on Article 114 of the Treaty on the Functioning of the European Union (TFEU), **the cumulative effects of designation, supplier listing, conditions for use or prohibition-type measures, together with their reliance on non-technical considerations, may resemble measures falling within the scope of the Union's common commercial policy under Article 207 TFEU** or broader foreign and security policy considerations under Article 24 TEU. Attention should therefore be paid to ensuring that measures adopted pursuant to this framework remain sufficiently linked to internal market harmonisation objectives, proportionate, legally predictable and respectful of Member States' competences, including national security responsibilities pursuant to Article 4(2) TEU.

7.3. Scope of Key ICT Assets and Coverage of ICT Services

Eurosmart notes that the current definition of "ICT assets", which serves as the basis for the notion of "key ICT assets", appears primarily focused on hardware and software assets. **As a result, certain ICT services and ICT processes, including cloud services, SaaS, PaaS, IaaS and archiving services, may fall outside the scope of mechanisms applicable to key ICT assets**, despite their critical importance for cybersecurity, operational resilience and digital sovereignty.

In light of the increasing reliance on service-based and operational ICT environments, greater clarity should therefore be ensured regarding the treatment of ICT services and ICT processes within the trusted ICT supply chain framework, in order to avoid regulatory gaps and future-proof approach. Eurosmart therefore supports clarifying the relevant definitions and provisions of the Regulation to explicitly cover ICT services and ICT processes where they are relevant to the protection of key ICT assets, critical infrastructures or sensitive operational environments.

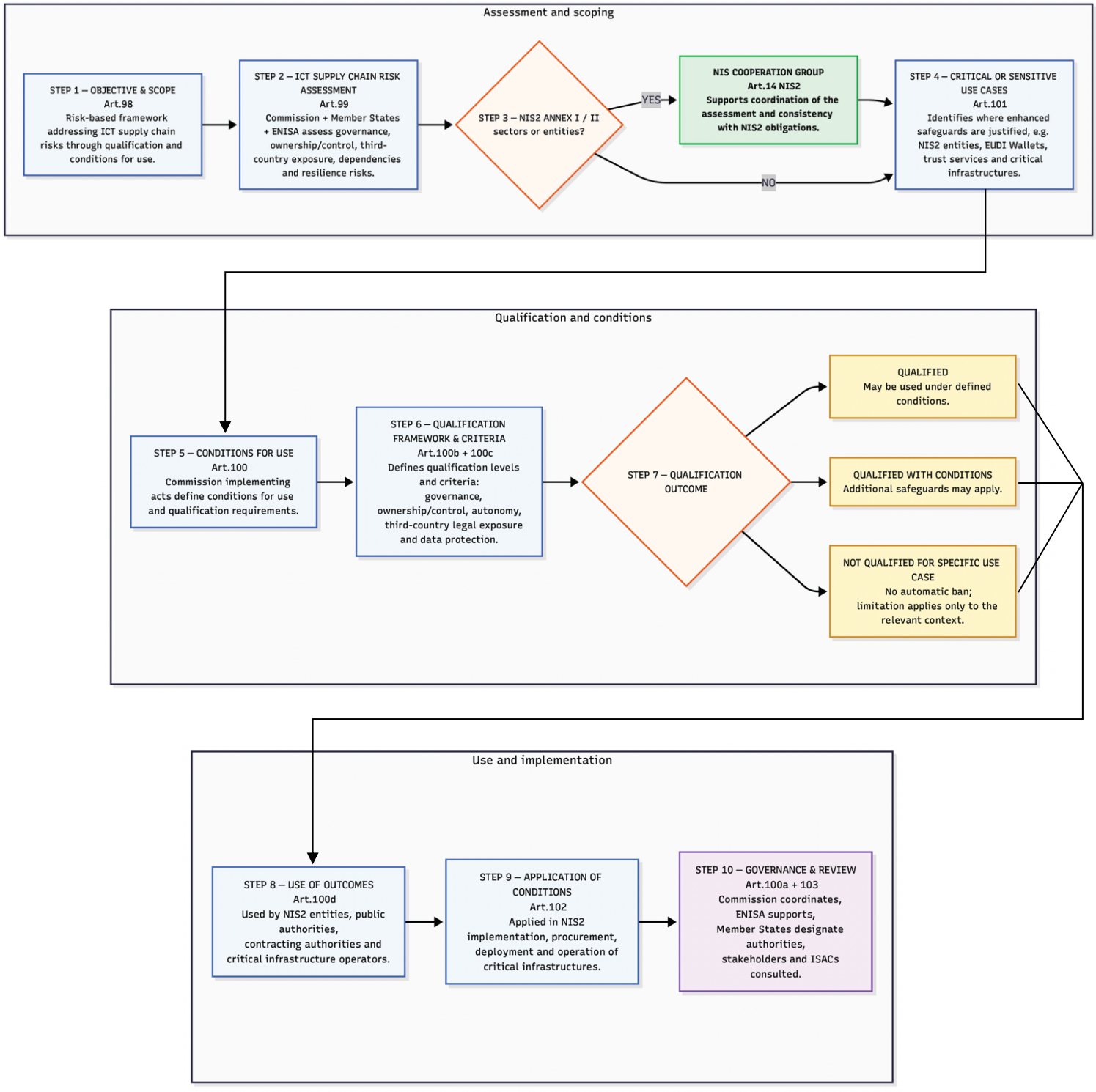
7.4. Proposal for a Risk-Based Qualification Approach

Eurosmart proposes a shift towards a structured, risk-based framework centred on the identification of critical and sensitive use cases. **Rather than targeting suppliers as such, this approach enables the qualification of ICT products, ICT services, ICT processes and providers for specific contexts of use, based on objective and proportionate criteria**. The framework provides for the qualification of ICT products, ICT services, ICT processes and suppliers in relation to specific contexts of use, thereby ensuring legal certainty, predictability and consistency with Union law, including Directive (EU) 2022/2555 and Regulation (EU) 2016/679. It also preserves the integrity of the internal market and the role of Member States by avoiding unjustified or disproportionate restrictions.

Such a qualification-based approach should be supported by a clear and robust governance framework involving the European Commission, Member States, ENISA and relevant stakeholders. Structured cooperation and consultation mechanisms should ensure that risk assessments, the identification of use cases and the definition of conditions for use are conducted in a transparent, consistent and technically informed manner.

This approach allows non-technical cybersecurity risks, including those related to third-country exposure, supply chain dependencies and systemic vulnerabilities, to be addressed in a proportionate and operational manner, while ensuring a clear distinction from the technical certification framework established under Title III.

Eurosmart's proposal for Title IV - Risk-Based ICT Supply Chain Qualification Framework



Annex - Proposed Amendments to CSA2

1. Recital 42

To support the implementation of Union policies and preparation of potential standardisation activities, ENISA should contribute to the development and evaluation of cryptographic algorithms, in particular in the area of post-quantum cryptography.

[ADDED -] ENISA should support the transition to post quantum cryptography by identifying priority use cases and sectors, ICT products or ICT services, assessing gaps, defining migration approaches, including through crypto agility, and contributing to relevant standards and technical specifications, including, where applicable, the development and maintenance of European cybersecurity certification schemes. Such support should be carried out in consistency with Commission Recommendation (EU) 2024/1101 and with the work undertaken by Member States, including national strategies and coordination mechanisms.]

[ADDED -] Likewise, ENISA should support the uptake of new cryptographic techniques supporting privacy which may be useful for instance in the context of digital identity or the EUDI Wallet by contributing to the development and evaluation of cryptographic algorithms, contributing to relevant standards and technical specifications, including, where applicable, the development and maintenance of European cybersecurity certification schemes. Such support should be carried out in consistency with Commission Recommendation (EU) 2024/1101 and with the work undertaken by Member States, including national strategies and coordination mechanisms.]

Rationale

Introduces new operational perspectives:
Regarding the introduction of post quantum cryptography:

- recognising the need to identify priority use cases and sectors, ICT products and ICT services,
- addressing technical and standardisation gaps,
- addressing migration approaches including through crypto agility,
- and supporting the development of relevant standards and certification-related specifications.

Regarding new cryptographic techniques supporting privacy:

- recognising the need to support new digital usages, in particular in the context of digital identity and EUDI Wallet,
- addressing technical and standardisation gaps,
- and supporting the development of relevant standards and certification-related specifications.

2. Article 47 - Fees

Add the following paragraph:

Fees shall remain transparent, proportionate and strictly limited to what is necessary to fund the activities referred to in paragraphs 2, 3 and 4, without generating surplus. They should be linked to clearly defined maintenance, development and support activities, including indicative timelines. Fee structures shall ensure predictability for economic operators, in particular SMEs, and shall not create barriers to entry or discourage participation in European cybersecurity certification schemes.

Rationale:

- These fees shall not become a mean for ENISA to make profit/generate surplus on third parties exceeding what is strictly necessary to fund the expenses referred in paragraph 2, 3 and 4 as it would entail substantial detrimental consequences:

3. Article 53 - Transparency and consultation

Extend paragraph 3:

- **Transparency shall cover not only access to documents but also provide visibility on the lifecycle of schemes, including maintenance activities, technical specifications, transition arrangements and updates.**
- **A traceable process for stakeholder input shall be ensured, while preserving confidentiality and security-sensitive information.**

4. Article 73 - Union rolling work programme

Add a new paragraph:

- **The rolling work programme shall prioritise schemes based on security criticality and market impact, including in particular:**
  - **Security-critical hardware components and embedded systems**
  - **Cryptographic components and solutions supporting post-quantum cryptography and crypto-agility**
  - **Digital identity and trust services**
  - **IoT, industrial control systems, cloud and edge infrastructures**

5. Article 18 - Standardisation, technical specifications and guidance

Article 18(3)

ENISA shall contribute to the development and evaluation of cryptographic algorithms

[ADDED including post-quantum cryptography and new cryptographic techniques supporting privacy]

[ADDED: and shall support the development, assessment and adoption of relevant standards and technical specifications on cryptographic algorithms, taking into account interoperability, security, feasibility, technological maturity and industry readiness]

[ADDED: Regarding post quantum cryptography, support the development, assessment and adoption of relevant standards and technical specifications for the introduction of post quantum cryptography in use cases and sectors, ICT products and ICT services taking into account interoperability, migration feasibility, technological maturity and industry readiness.]

[ADDED: ENISA shall, within its mandate, provide technical advice and guidance to the Commission and to the Member States in support of the transition towards post-quantum cryptography, including as regards the identification of relevant use cases and sectors, ICT products and ICT services, the assessment of technical and operational challenges, and the development of migration approaches, including through crypto-agility.]

[ADDED: In carrying out those tasks, ENISA shall ensure consistency with, and support the implementation of, the work undertaken by Member States pursuant to (1) Commission Recommendation (EU) 2024/1101, in particular with regard to national transition strategies, coordination mechanisms and indicative timelines and (2) regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.]

Rationale

Strengthen ENISA's role in relation to migration to post quantum cryptography and new cryptographic techniques supporting privacy within the framework of its existing mandate, while ensuring consistency with regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (i.e.; EUDI Wallet).

Ensures that ENISA's activities:

- are aligned with the Member States-led approach to the transition towards post-quantum cryptography;
- are aligned with the Member States and Commission-led activities regarding the EUDI Wallet framework;

The amendment further ensures that ENISA's contribution remains:

- technical in nature,
- complementary to Member States' and Commission's responsibilities.

6. Article 74 - Preparation of Candidate Schemes

Article 74(2)

ENISA shall prepare the candidate scheme in close cooperation with the European Cybersecurity Certification Group. For that purpose, ENISA may establish ad hoc working groups composed of experts from Member States, Union institutions, bodies, offices and agencies and other relevant stakeholders.

[ADDED: Where ENISA establishes such ad hoc working groups, it shall ensure that the development of candidate schemes includes appropriate intermediary consultation steps

with relevant stakeholders beyond the members of those working groups, allowing for broader input prior to the finalisation of the candidate scheme.

The selection of experts shall be primarily based on demonstrated technical competence and relevant domain expertise. While inclusiveness and balanced representation are important, they shall not compromise the effectiveness, technical quality, and security relevance of expert contributions.]

Rationale

- Ensures transparency and inclusiveness in scheme development, not only maintenance
- Prevents closed or expert-only processes ("black box")
- Anchors stakeholder consultation at the **earliest stage (design phase).** Fully consistent with Recital 90 (stakeholder involvement)

7. Article 75 - Maintenance of European Cybersecurity Certification Schemes

Article 75(2)

ENISA, in cooperation with the Commission and supported by the European Cybersecurity Certification Group (ECCG) and its relevant maintenance sub-group, shall ensure the maintenance of European cybersecurity certification schemes, including in view of the possible review of such schemes by the Commission.

ENISA shall cooperate and exchange information with relevant Union entities and groups ~~in relation to maintenance activities~~ **[ADDED: , as well as with relevant stakeholder groups, including, where appropriate, Information Sharing and Analysis Centres (ISACs), in relation to maintenance activities.]**

Article 75(3)

3. For the purpose of ensuring effective and technically robust maintenance of a European cybersecurity certification scheme, ENISA may, in accordance with the maintenance strategy referred to in paragraph 1, organise the ~~involvement~~ **[ADDED: structured involvement]** of relevant stakeholders, including through ~~ad hoc working groups~~ **[ADDED: sectoral liaison arrangements or, where appropriate, ad hoc working groups]**, with relevant stakeholder groups such as Information Sharing and Analysis Centres (ISACs), without prejudice to ENISA's responsibility for ensuring the maintenance of the scheme.**[ADDED: Where relevant stakeholder interaction cannot be clearly identified or where no established stakeholder ecosystem exists, ENISA may establish ad hoc working groups to ensure that the necessary technical expertise is mobilised.]**

Article 75(4)(c)

(c) interactions ~~with relevant stakeholders~~ **[ADDED: and, where relevant, the establishment of liaisons with relevant stakeholders]**, including ~~European and international standardisation organisations~~ **[ADDED: European or international standardisation organisations and Information Sharing and Analysis Centres (ISACs)]**, including for the purpose of making or receiving technical contributions.

Article 75(4) (g) (h) New

[ADDED:] (g) In carrying out the activities referred to in points (a) to (f), ENISA shall, where relevant, support the adaptation of European cybersecurity certification schemes to emerging cryptographic risks, including those arising from the development of quantum computing.

[ADDED:] (h) In particular, this may include the identification of relevant use cases and sectors, ICT products or ICT services, contributions to technical specifications and standards, and support to the development of transition approaches for the gradual adoption of post-quantum cryptography, including through crypto agility.

Article 75(5) New

[ADDED:]

5. ENISA shall ensure that maintenance activities and the development of European cybersecurity certification schemes include appropriate intermediary consultation steps, allowing for broader stakeholder input prior to the finalisation of technical specifications, maintenance documents or certification schemes.

Rationale

- Provides a clear legal basis for structured stakeholder involvement
- Explicitly recognises ISACs as operational contributors
- Ensures ENISA:
  - leverages existing ecosystems
  - retains flexibility (ad hoc groups only where needed)
- Avoids duplication of well-functioning industry - public/private structures
- Introduces **consultation safeguards** across schemes' lifecycle

Moreover, new paragraphs (g) and (h) clarify that **PQC is addressed within the existing maintenance activities of certification schemes**. They also ensure that ENISA may support the adaptation of schemes through existing mechanisms, including technical specifications, standardisation and stakeholder engagement, without creating additional obligations.

8. Article 76 - Withdrawal of European cybersecurity certification schemes

Add a new paragraph:

- **The withdrawal of a European cybersecurity certification scheme shall remain exceptional and subject to a thorough impact assessment. Appropriate transition measures shall be ensured, including:**
  - **Continued validity of existing certificates for their full duration**
  - **Sufficient transition periods**
  - **Availability of alternative certification paths**

- **Such measures shall preserve legal certainty and market continuity.**

9. Article 77 - Technical specifications

Add new paragraph:

- Technical specifications shall be based on **recognised European or international standards** or developed through **open and transparent multi-stakeholder processes**.
- ENISA's role in relation to technical specifications shall remain limited to **coordination and facilitation** and shall not introduce any **de facto approval or oversight function** over certification activities, in order to preserve impartiality and role separation.

10. Article 80 - Security objectives of European cybersecurity certification schemes

Article 80(1)

A European cybersecurity certification scheme shall pursue, as applicable, the following security objectives:

[ADDED: (ea) where appropriate, elements supporting the adaptation to evolving cryptographic requirements, including crypto-agility considerations.]

[ADDED: (zz) Support and are in line with the Member States-led approach for the implementation of DIRECTIVE (EU) 2022/2555, such as the one enshrined in Commission Recommendation (EU) 2024/1101.]

Rationale

Provision allowing certification schemes to address new needs stemming from the Member States-led approach for the implementation of NISD2, such as the introduction of post quantum cryptography.

Provides flexibility while avoiding over-specification, as the implementation of such adaptations is addressed through maintenance activities.

Article 80(2) - Security Objectives

The Commission is empowered to adopt delegated acts in accordance with Article 119 to amend paragraph 1 of this Article by adding or modifying security objectives in order to ensure that they reflect the latest technological development **[ADDED: including, where relevant, objectives ensuring resilience against evolving cryptographic risks, protection against advanced logical, side-channel and physical attacks]** and new related threats as well as adoption of new Union legislation setting out the demonstration of compliance and the presumption of conformity through European cybersecurity certification with relevant cybersecurity requirements of that legislation.

Rationale

Maintains high-level coherence with: Article 75 (implementation).

11. Article 82 - Assurance and Evaluation Levels

Article 82(7)(c)

(c) an assessment of the resistance of the ICT products, ICT services, ICT processes, managed security services or entities to skilled attackers, ~~using , where relevant, penetration testing~~.

[ADDED: For ICT products, such assessment shall include penetration testing.]

[ADDED: For ICT services, ICT processes, managed security services or entities, where penetration testing is not appropriate, substitute evaluation activities with an equivalent effect shall be undertaken.]

[ADDED: For assurance level "high", evaluation activities shall be commensurate with realistic and advanced attacker capabilities, taking into account, where relevant, logical, side-channel, physical and hardware-oriented attack vectors.]

[ADDED: The depth and scope of evaluation activities shall be explicitly linked to the applicable threat model, security objectives and intended use of the ICT products, ICT services, ICT processes, managed security services or entities, in order to ensure a consistent and high level of assurance across European cybersecurity certification schemes.]

Rationale

- Removes discretion weakening "High" assurance level
- Ensures mandatory penetration testing for ICT products
- Preserves flexibility for:
  - ICT processes
  - services
- Aligns with:
  - state-of-the-art evaluation practices
  - market expectations for high assurance

12. Article 87 - International Recognition

Article 87(1)

The Commission may adopt implementing acts to determine that the requirements of a cybersecurity certification scheme of a third country or of an international organisation are equivalent to those of a European cybersecurity certification scheme.

~~In such cases, certificates issued under those schemes shall be recognised as equivalent to certificates issued under European cybersecurity certification schemes.~~

[ADDED: In assessing such equivalence, the Commission shall ensure that appropriate technical expert consultation takes place, including, where relevant, consultation of ENISA-supported ad hoc working groups and relevant stakeholder organisations such as Information Sharing and Analysis Centres (ISACs).]

[ADDED: The Commission shall also take into account the existence of structured technical cooperation, including participation in ENISA maintenance activities, ad hoc working groups or stakeholder cooperation structures related to the relevant certification scheme.]

Article 87(2a) - New

[ADDED:]

2a. For the purpose of assessing equivalence pursuant to paragraph 1, the Commission shall, with the support of ENISA and in consultation with the European Cybersecurity Certification Group, organise a technical review of the supervisory, accreditation and conformity assessment arrangements applicable under the relevant third-country scheme.

The findings of such review shall inform the Commission's decision under paragraph 1.

Rationale

- Reinforces technical integrity of equivalence decisions
- Reduces risk of political influence and/or commercial bias
- Introduces:
  - expert consultation
  - structured technical review
- Addresses gap vs EU internal peer review (Article 89) while preserving comitology approach

13. Article 89 - Peer Review

3. Peer review shall assess [...]

[ADDED:]

(e) where applicable, whether the authorities or bodies involved in the issuance, supervision or review of European cybersecurity certificates at assurance level "high" possess the appropriate technical expertise, operational capabilities and sufficient skilled personnel necessary to perform advanced cybersecurity evaluations, including vulnerability analysis, penetration testing and other high-assurance assessment activities.

Rationale

This amendment restores and modernises an important safeguard previously reflected in Regulation (EU) 2019/881 concerning the assessment of technical expertise for assurance level "high" certification activities.

14. Article 94 - Peer reviews and oversight of conformity assessment bodies

[ADDED: 4a. Measures adopted pursuant to paragraph 4 shall remain exceptional, duly justified and proportionate, and shall not create an additional supervisory layer beyond

existing accreditation, notification and certification frameworks. Such measures shall respect due process, preserve the competences of national authorities, avoid unnecessary disruption of ongoing certification activities and ensure continuity, predictability and legal certainty for economic operators and certification stakeholders.]

Rationale

This amendment clarifies that Union-level oversight and corrective measures concerning conformity assessment bodies should remain proportionate, exceptional and respectful of existing national accreditation and notification frameworks. It also aims to preserve legal certainty, continuity of certification activities and the respective roles of national authorities and economic operators.

Amendments related to Title IV - Chapter 1

15. New Recital - Clarification on Title IV

[ADDED:]

(XX) The mechanisms established under Title IV are intended to address risks related to ICT supply chains, including non-technical cybersecurity risks, systemic dependencies and risks arising from governance, operational or third-country legal exposure. Those mechanisms should remain distinct from the technical certification framework established under Title III and should not constitute conformity assessment, certification or presumption of conformity within the meaning of Union harmonisation legislation.

The measures established pursuant to this Title should be based on structured risk assessment, objective and proportionate qualification criteria, and conditions for use adapted to the level of criticality and sensitivity of specific use cases. They should support a risk-based and predictable framework enabling the assessment of the suitability of ICT products, ICT services, ICT processes and suppliers thereof for specific contexts, while preserving consistency with Union law, including Directive (EU) 2022/2555, internal market principles and relevant data protection requirements.

The implementation of this Title should ensure transparency, proportionality, legal certainty and appropriate stakeholder involvement.

Rationale

- Clarifies that Title IV establishes a risk-management and suitability framework, distinct from the technical certification and conformity assessment framework under Title III.
- Prevents confusion between technical cybersecurity certification and broader geopolitical or non-technical risk-management measures.
- Introduces a structured, risk-based and use-case-oriented approach based on objective and proportionate qualification criteria.
- Ensures that conditions for use are adapted to the criticality and sensitivity of specific use cases.

- Strengthens transparency, proportionality, legal certainty and predictability for economic operators and Member States.
- Preserves consistency with Union law, including Directive (EU) 2022/2555, internal market principles and relevant data protection requirements.

16. Article 2 - Definitions

Article 2 - New

[ADDED: (XX) 'qualification criteria' means objective, transparent and proportionate requirements used to assess the ability of ICT products, ICT services, ICT processes or suppliers thereof to be used in specific contexts, taking into account cybersecurity, governance, and legal risk factors, including those related to third-country exposure.]

[ADDED: (XXa) 'critical or sensitive ICT use case' means a deployment context, operational environment, infrastructure, ICT product, ICT service, ICT process or activity involving ICT products, ICT services or ICT processes where heightened cybersecurity, resilience, operational autonomy, governance or supply chain safeguards may be justified due to the potential impact of disruption, compromise, systemic dependency, unauthorised access or operational interference on essential or important services, public security, economic stability or the functioning of the internal market.]

Rationale - Article 2

This amendment introduces clear definitions of both "qualification criteria" and "critical or sensitive ICT use case", thereby improving legal certainty, technological neutrality and consistency across the Regulation.

1. The definition of **"qualification criteria"** clarifies that the framework is based on the assessment of suitability for use in specific operational contexts, rather than on certification, designation or exclusion mechanisms, and aligns with Union risk-based approaches. This notion is used in particular in proposed articles 100, 100b and 100c relating to conditions for use and qualification requirements.
2. The introduction of the notion of **"critical or sensitive ICT use case"** also reflects the need to move beyond a narrow *(critical) asset-based approach* focused solely on hardware or software components. In particular, it takes into account the increasing importance of ICT services, ICT processes, cloud environments and operational ecosystems in modern digital infrastructures alongside ICT products. This approach ensures that the framework remains adaptable to evolving technologies and deployment models, while avoiding regulatory gaps affecting ICT services or operational environments that may be critical from a cybersecurity and resilience perspective. It also enables a more proportionate, operational and context-based assessment of supply chain risks. The concept is notably used in proposed articles 100, 100d and 101 concerning the identification of sensitive deployment contexts and the application of conditions for use.

17. Article 98 - Objective and Scope

Article 98 - Full rewording

1. The trusted ICT supply chain framework shall provide for the identification and management of risks related to ICT supply chains, including non-technical cybersecurity risks, and for the qualification of ICT suppliers and service providers for specific use cases, with a view to ensuring a high level of cybersecurity, resilience and trust within the Union.
2. The framework shall ensure that ICT products, ICT services, ICT processes and suppliers thereof can be used in the Union under transparent, proportionate and predictable conditions, taking into account the level of criticality and sensitivity of the use case.
3. Measures adopted pursuant to this Chapter shall be based on a structured assessment of risks and shall result, where appropriate, in the definition of conditions for use and qualification criteria.
4. This Chapter shall complement and remain consistent with:
    a) European cybersecurity certification schemes established under Title III;
    b) Union legislation on cybersecurity risk management, including Directive (EU) 2022/2555;
    c) Union rules on public procurement;
    d) relevant sectoral or Union-level risk assessment frameworks.
5. The provisions laid down in this Chapter shall not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity in ICT supply chains, provided that such provisions are consistent with their obligations under Union law.

Rationale - Article 98

Clarifies the framework as a **risk-based and qualification-driven mechanism**, ensuring that supply chain risks are addressed through proportionate conditions for use rather than restrictive approaches (risk of ban under political decisions).

It introduces the notion of **qualification of actors for specific use cases**, **ensuring a structured and predictable framework consistent with the internal market.**

18. Article 99 - ICT Supply Chain Risk Assessment

Article 99 - Restructuring

The Commission, in cooperation with Member States, ENISA and relevant stakeholders, shall identify and assess risks related to ICT supply chains, including non-technical cybersecurity risks.

[ADDED: 1. The Commission, in cooperation with Member States, ENISA and the European Cybersecurity Certification Group, shall identify and assess risks related to ICT supply chains at Union level, including non-technical cybersecurity risks.]

[ADDED 2. Where ICT supply chain risk assessments concern sectors or entities referred to in Annex I or Annex II to Directive (EU) 2022/2555, the Cooperation Group established pursuant to Article 14 of that Directive shall support the coordination of the identification and assessment of such risks, in cooperation with the Commission, Member States, ENISA and the European Cybersecurity Certification Group.]

[ADDED: 3. The assessment shall be based on objective, transparent and proportionate criteria, taking into account, where relevant:]

[ADDED: (a) the governance structure of ICT suppliers and service providers, including risks of undue influence;]

[ADDED: (b) the ownership and control structure, including exposure to third-country legal frameworks;]

[ADDED: (c) the existence of legal or practical obligations requiring disclosure of vulnerabilities or sensitive information to public authorities of third countries;]

[ADDED: (d) the risks related to the extraterritorial application of third-country laws, including obligations to disclose or provide access to data, and their potential incompatibility with Union law, in particular Regulation (EU) 2016/679;]

[ADDED: (e) the availability of effective judicial remedies and independent oversight mechanisms;]

[ADDED: (f) substantiated information on malicious cyber activities linked to entities operating under the jurisdiction of a third country, and the level of cooperation with Union authorities;]

[ADDED: (g) existing practices in a third country, demonstrated by independent sources, where ICT products, ICT services or ICT processes contain undocumented backdoors allowing remote access or remote control;]

[ADDED: (h) the existence of laws in a third country requiring entities under its jurisdiction to block or limit the purchase or access to ICT products, ICT services or ICT processes, or to block, restrict, limit or tamper with the use of ICT products, ICT services or ICT processes;]

[ADDED: (i) existing practices in a third country, demonstrated by independent sources, requiring entities under its jurisdiction to block or limit the purchase or access to ICT products, ICT services or ICT processes, or to block, restrict, limit or tamper with the use of ICT products, ICT services or ICT processes;]

[ADDED: (j) the existence of laws in a third country requiring entities under its jurisdiction to give access to data from a foreign entity they store or process to public authorities of that third country;]

[ADDED: (k) existing practices in a third country, demonstrated by independent sources, requiring entities under its jurisdiction to give access to data from a foreign entity they store or process to public authorities of that third country;]

[ADDED: (l) the level of dependency on specific suppliers or technologies within critical ICT supply chains;]

[ADDED: (m) the potential impact of disruption or compromise on essential services or critical infrastructure;]

[ADDED: (n) the ability of ICT suppliers to ensure the integrity and security of their products and services throughout their lifecycle;]

[ADDED: (o) relevant information stemming from Union-level coordinated risk assessments or reports by Member States or international organisations.]

[ADDED: 4. ENISA shall support the Commission in developing and maintaining methodologies for the assessment of such risks.]

[ADDED: 5. The Commission shall ensure appropriate consultation of relevant stakeholders, including industry representatives, certification bodies and Information Sharing and Analysis Centres (ISACs).]

[ADDED: 6. The results of the assessment shall inform the establishment of conditions for use pursuant to Article 100.]

Rationale - Article 99

The initial mechanisms established under this Article overlap with the coordinated security risk assessments already provided for under Article 22 of Directive (EU) 2022/2555 and substantially affect the governance framework established under the NIS2 Directive.

In order to ensure legal clarity, consistency and coherence with the Union cybersecurity acquis, the provisions relating to coordinated ICT supply chain risk assessments should be articulated consistently with the framework established under Directive (EU) 2022/2555, including through targeted amendments where appropriate.

The new proposed ICT supply chain risk assessment shall serve as a structured mechanism for identifying risks relevant to the establishment of proportionate qualification criteria and conditions for use applicable to sensitive ICT use cases.

In addition, a definition of "**supply chain**" – drawn from the one introduced in the CSA2 in article 2(40) for ICT supply chain - should be introduced in Directive (EU) 2022/2555 in order to ensure consistent interpretation and implementation across Member States.

19. Article 100 - Conditions for Use and Qualification

Article 100 - Full rewording

1. On the basis of the assessment carried out pursuant to Article 99, the Commission shall establish, by means of implementing acts, conditions for the use of ICT products, ICT services, ICT processes or suppliers thereof in specific contexts, taking into account the level of criticality and sensitivity of the use case.
2. The implementing acts referred to in paragraph 1 shall define:

   (a) the applicable conditions for use, including, where appropriate, governance, operational autonomy, localisation, access control or participation safeguards proportionate to the level of criticality and sensitivity of the relevant use case;

   (b) the qualification criteria enabling the assessment of ICT suppliers, service providers or categories thereof for specific use cases;

(c) where appropriate, differentiated requirements depending on the level of criticality and sensitivity of the use case.

3. The qualification criteria established pursuant to this Chapter shall be defined in accordance with Article 100(c).
4. ENISA shall support the Commission in the preparation of the implementing acts referred to in paragraph 1, including through technical guidance and in consultation with the European Cybersecurity Certification Group and relevant stakeholders, including Information Sharing and Analysis Centres (ISACs) and ad-hoc working groups created for the European cybersecurity schemes' maintenance.
5. The development and application of conditions for use and qualification criteria shall ensure transparency, inclusiveness and proportionality.
6. Conditions established pursuant to this Article shall remain distinct from and shall not undermine European cybersecurity certification schemes established under Title III.

Rationale - Article 100

This amendment establishes a structured framework for defining conditions for use and qualification requirements applicable to ICT products, ICT services, ICT processes and suppliers thereof in critical or sensitive use cases identified pursuant to Article 101.

The provision ensures that measures adopted under this Chapter are based on objective risk assessments and proportionate qualification criteria adapted to the level of criticality and sensitivity of the relevant use case.

It also reinforces transparency, stakeholder involvement and consistency with Directive (EU) 2022/2555 and European cybersecurity certification schemes established under Title III, while preserving the distinction between qualification mechanisms and technical certification processes.

20. Article 100a (NEW) - Qualification Mechanism

1. The Commission shall ensure the coherent implementation and coordination of the qualification framework established pursuant to this Chapter, in close cooperation with Member States, ENISA and the European Cybersecurity Certification Group.

2. ENISA shall support the Commission and Member States by:

(a) contributing to the development of methodologies, technical guidance and qualification criteria;

(b) supporting the assessment of risks related to ICT supply chains and sensitive use cases;

(c) facilitating cooperation and information exchange among competent authorities and relevant stakeholders;

(d) supporting the periodic review and adaptation of qualification conditions.

3. Member States shall designate one or more competent authorities responsible for the supervision and implementation of qualification-related measures under this Chapter.

4. The Commission shall ensure structured consultation of relevant stakeholders, including industry representatives, certification bodies, standardisation organisations and Information Sharing and Analysis Centres (ISACs).

5. Where appropriate, the Commission or ENISA may establish expert groups, ad hoc working groups or sectoral cooperation mechanisms in support of the implementation of this Chapter.

Rationale

This amendment establishes a structured and risk-based Union qualification mechanism for ICT products, ICT services, ICT processes and suppliers thereof used in critical or sensitive ICT use cases identified pursuant to Article 101.

The mechanism enables the definition of proportionate conditions for use and differentiated qualification outcomes adapted to the level of criticality, sensitivity and operational risk associated with specific use cases.

21. Article 100b (New) - Governance and Competent Authorities

1. The Commission shall establish, by means of implementing acts, a Union framework for the qualification of ICT products, ICT services, ICT processes and suppliers thereof for specific critical or sensitive use cases identified pursuant to Article 101.
2. The qualification framework shall provide for:

(a) qualification categories and, where appropriate, differentiated qualification levels reflecting the level of criticality, sensitivity, risk exposure and operational requirements associated with the relevant use case;

(b) conditions for use applicable to qualified ICT products, ICT services, ICT processes or suppliers thereof;

(c) procedures for granting, reviewing, suspending or withdrawing qualification outcomes;

(d) periodic review mechanisms ensuring that qualification outcomes remain aligned with evolving risks, technological developments and operational circumstances.

3. Qualification pursuant to this Chapter shall not constitute a European cybersecurity certification scheme within the meaning of Title III and shall remain distinct from conformity assessment activities established under Union harmonisation legislation.

4. Qualification outcomes established pursuant to this Chapter shall be based on objective, transparent and proportionate criteria and shall not result in unjustified restrictions on the internal market.

Rationale

This amendment establishes a coherent governance framework for the implementation and supervision of the qualification mechanism established under this Chapter.

It clarifies the respective roles of the Commission, Member States, ENISA and relevant stakeholders in the development, implementation and review of qualification requirements and conditions for use applicable to critical or sensitive ICT use cases.

The provision ensures that the qualification framework may provide for differentiated qualification categories and levels proportionate to the level of criticality, sensitivity and risk exposure associated with the relevant use case, while preserving flexibility and technological neutrality.

It also reinforces coordination and consistency across the Union, while ensuring appropriate stakeholder consultation and alignment with existing Union cybersecurity frameworks, including Directive (EU) 2022/2555 and European cybersecurity certification schemes established under Title III.

The amendment further ensures that the qualification framework remains distinct from conformity assessment and certification mechanisms under Union harmonisation legislation and supports a transparent, proportionate and predictable approach to ICT supply chain risk management.

22. Article 100c (New) - Qualification Criteria

1. Qualification criteria established pursuant to this Chapter shall build upon the risk assessments carried out pursuant to Article 99.

2. Qualification criteria established pursuant to this Chapter shall be objective, transparent, proportionate and risk-based.

3. Qualification criteria may include, where relevant:

(a) cybersecurity capabilities and risk management measures;

(b) governance structure and safeguards against undue influence, including organisational, legal and operational independence guarantees;

(c) ownership and control transparency, including the identification of direct or indirect control, significant influence or dependency relationships;

(d) supply chain resilience, dependency management and continuity capabilities;

(e) the ability to ensure the integrity, confidentiality, availability and security of ICT products, ICT services and ICT processes throughout their lifecycle;

(f) compliance with Union law, including cybersecurity, data protection and data governance requirements;

(g) accountability and openness to scrutinity;

(h) protection against risks arising from the extraterritorial application of third-country laws, including risks of access, disclosure or transfer obligations incompatible with Union law;

(i) guarantees relating to operational autonomy, access control, privileged access management, auditability and incident response capabilities;

(j) the existence of effective legal, technical and organisational measures ensuring protection against unauthorised access by third-country authorities or entities;

(k) the localisation and governance of sensitive operations, including where appropriate the localisation of security-sensitive functions, administration, support or data processing activities within the Union;

(l) the protection of personal and non-personal data, including commercially sensitive data, trade secrets and data relating to legal persons processed, stored or managed by the relevant ICT products, ICT services or suppliers thereof;

(m) the ability to operate under fair, reasonable and non-discriminatory conditions consistent with Union law and internal market principles.

(n) alignment with recognised European or international standards and, where appropriate, European cybersecurity certification schemes established under Title III.

(o) the protection against blocking or limitation of the purchase or access to ICT products, ICT services or ICT processes, or blocking, restriction, limitation or tampering with the use of ICT products, ICT services or ICT processes.

(p) the protection against undocumented backdoors allowing remote access or remote control of ICT products, ICT services or ICT processes.

(q) protection against the compromising of the integrity and security of upstream supply chain of the ICT products, ICT services or ICT processes

4. Qualification criteria shall be adapted to the level of criticality and sensitivity of the relevant use case and shall avoid imposing unnecessary or disproportionate obligations.

5. Qualification criteria shall be reviewed periodically considering technological developments, evolving threats and operational experience.

Rationale

This amendment establishes a structured set of qualification criteria intended to support the assessment of the suitability of ICT products, ICT services, ICT processes and suppliers thereof for critical or sensitive use cases identified pursuant to Article 101.

The criteria combine governance, operational resilience and legal risk considerations in order to address both technical and non-technical cybersecurity risks related to ICT supply chains, including risks arising from systemic dependencies, undue influence, operational control and exposure to third-country legal frameworks.

The provision ensures that qualification criteria remain objective, transparent, proportionate and risk-based, while allowing adaptation to the level of criticality and sensitivity of the relevant use case. It also reinforces consistency with Union law, including cybersecurity, data protection and internal market requirements, and takes into account the need to protect both personal and non-personal data, including commercially sensitive data and data relating to legal persons.

23. Article 100 d (New) - Use of Qualification Outcomes

1. Qualification outcomes established pursuant to this Chapter may be used by:

(a) entities subject to Directive (EU) 2022/2555;

(b) public authorities and contracting authorities;

(c) operators of critical or sensitive ICT infrastructures;

(d) other entities identified pursuant to Union or national law, for the purposes of ICT supply chain risk management, procurement, deployment and compliance with cybersecurity obligations relating to critical or sensitive use cases.

2. Member States shall ensure that the application of qualification outcomes remains proportionate, risk-based and consistent with Union law, including internal market principles.

3. Qualification outcomes shall not automatically result in general prohibitions or exclusions outside the specific contexts and use cases for which they are established.

4. The application of qualification outcomes shall preserve the flexibility of entities subject to Directive (EU) 2022/2555 to conduct case-by-case risk assessments where appropriate.

5. The Commission and Member States shall ensure consistency between the implementation of this Chapter and Union legislation relating to cybersecurity, public procurement, data protection and critical infrastructure protection.

Rationale

This amendment clarifies the operational use and legal effects of qualification outcomes established under this Chapter.

It ensures that qualification outcomes may support ICT supply chain risk management, procurement and deployment decisions in sensitive or critical use cases, while preserving a proportionate, risk-based and context-specific approach.

The provision ensures that qualification outcomes are applied only in relation to the relevant use cases and levels of criticality identified pursuant to Article 101. It also preserves the flexibility of entities subject to Directive (EU) 2022/2555 to perform case-by-case risk assessments and implement appropriate cybersecurity risk management measures.

The amendment further reinforces consistency with Union law, including Directive (EU) 2022/2555, internal market principles, public procurement rules and Union data protection requirements, while ensuring that the framework remains distinct from technical certification schemes established under Title III.

24. Article 101 - Critical and Sensitive Use Cases

Article 101 - Substantial restructuring

~~1. The Commission... [general mechanism wording]~~

[ADDED: 1. The Commission, in cooperation with Member States and ENISA, shall identify categories of ICT use cases which are considered critical or sensitive for the purposes of this Chapter. The identification of critical or sensitive ICT use cases shall serve as the basis for determining whether enhanced qualification criteria or specific conditions for use established pursuant to Article 100 are justified in light of the level of cybersecurity, resilience, operational or systemic risk associated with the relevant context.]

~~2. The mechanism shall...~~

[ADDED: 2. The identification shall take into account:]

[ADDED: (a) the role of ICT products, ICT services, ICT processes in the provision of essential or important services, in particular as referred to in Directive (EU) 2022/2555, including Articles 3 and 6 thereof;]

[ADDED: (b) the potential impact of disruption or compromise on public security, safety or economic stability;]

[ADDED: (c) the level of dependency on specific ICT suppliers or technologies;]

[ADDED: (d) the sensitivity of data processed or transmitted, including where such data may be subject to access or transfer obligations under third-country legal frameworks;]

[ADDED: (e) the risks related to the extraterritorial application of third-country laws, including obligations to disclose or provide access to data, and their potential incompatibility with Union law, in particular Regulation (EU) 2016/679;]

[ADDED: (f) relevant Union legislation, including Directive (EU) 2022/2555,]

[ADDED: (g) the existence of heightened cybersecurity, resilience, operational autonomy or governance requirements associated with specific sectors or infrastructures,]

[ADDED: (h) whether the use case relates to digital identity infrastructures, trust services, EUDI Wallets or European Business Wallets, payment infrastructure requiring enhanced cybersecurity, resilience and governance guarantees.]

[ADDES: (i) the existence of heightened strategic autonomy, sovereignty or resilience requirements associated with specific ICT infrastructures, services or governance ecosystems.]

[ADDED: 3. The categories of critical or sensitive ICT use cases shall be adopted and periodically reviewed by means of implementing acts.]

[ADDED: 4. The identified ICT use cases shall serve as a basis for the application of conditions for use established pursuant to Article 100 and shall not in itself result in the prohibition or exclusion of ICT products, ICT services, ICT processes or suppliers.]

Rationale - Article 101

Ensures alignment with NIS2 and GDPR and reinforces a **use-case-based, risk-driven approach**, including data sovereignty considerations.

It introduces a structured and use-case-based approach for the application of enhanced ICT supply chain safeguards.

Rather than relying on generalised supplier designations or broad exclusion mechanisms, the framework identifies specific ICT use cases where heightened cybersecurity, resilience, governance or operational autonomy requirements may be justified in light of the level of risk associated with the relevant context.

The identification of critical or sensitive ICT use cases serves as the operational basis for the application of proportionate qualification criteria and conditions for use established pursuant to Article 100. This approach ensures that enhanced safeguards are targeted, predictable and adapted to the criticality and sensitivity of the relevant use case, while preserving flexibility for entities subject to Directive (EU) 2022/2555 to conduct case-by-case risk assessments.

The provision also ensures consistency with Union cybersecurity, data protection and internal market frameworks, including Directive (EU) 2022/2555 and Regulation (EU) 2016/679, while taking into account risks related to systemic dependencies, operational resilience and exposure to third-country legal frameworks.

Particular attention should be paid to payment infrastructure, digital identity and trust infrastructures due to their systemic importance for the Digital Single Market and their reliance on high levels of operational trust, governance integrity and resilience.

25. Article 102 - Application of Conditions for Use

Article 102 - Full rewording

1. Conditions for use established pursuant to Article 100 shall be applied in relation to the use cases identified pursuant to Article 101.
2. Member States and relevant entities shall apply such conditions consistently when:

   (a) implementing obligations pursuant to Directive (EU) 2022/2555;

   (b) deploying ICT products, ICT services and ICT processes in the context of essential or important entities as referred to in Directive (EU) 2022/2555, or in use cases identified pursuant to Article 101;

   (c) conducting public procurement procedures involving ICT products, ICT services and ICT processes.
3. The application of conditions shall remain proportionate and shall not result in unjustified restrictions on the internal market.

Rationale - Article 102

Ensures operational application and anchors the framework in:

- NIS2 obligations,
- deployment decisions,
- procurement practices.

26. Article 103 - Governance, Implementation and Review

Article 103 - Full rewording

1. The Commission shall ensure that the development, implementation and review of this Chapter are carried out in close cooperation with Member States, ENISA and the European Cybersecurity Certification Group.

2. ENISA shall support the Commission in:

    (a) the development of risk assessment methodologies pursuant to Article 99;

    (b) the preparation of implementing acts pursuant to Article 100;

    (c) the monitoring and review of the framework.

3. The Commission shall ensure structured and timely consultation of relevant stakeholders, including industry representatives, certification bodies and Information Sharing and Analysis Centres (ISACs). Where appropriate, expert groups or ad hoc working groups may be established. Participation in advisory structures, expert groups or stakeholder consultation mechanisms established pursuant to this Chapter may, where sensitive ICT supply chain matters are concerned, be subject to appropriate transparency, independence, governance and conflict-of-interest safeguards, including safeguards relating to undue influence, operational autonomy and the protection of sensitive information.
4. Member States shall ensure consistent and proportionate application of conditions for use established pursuant to Article 100, including in the implementation of Directive (EU) 2022/2555 and in public procurement procedures.
5. The Commission shall monitor the implementation and impact of this Chapter and shall review and, where appropriate, update implementing acts, taking into account technological developments, evolving threats and stakeholder feedback.

Rationale - Article 103

Streamlines governance into a **single, coherent provision**, strengthening:

- ENISA's role,
- stakeholder involvement
- Member State coordination,
- continuous review.

Appropriate governance safeguards may be necessary in sensitive ICT supply chain contexts in order to preserve trust, independence and integrity in the preparation and implementation of Union-level measures.

27. [DELETED: Articles 104 to 109]

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

EUROSMART
The Voice of the Digital Security Industry

Square de Meeûs 35 | 1000 Brussels | Belgium
www.eurosmart.com