Open Regulatory Compliance

Contribution to the call for feedback of the Cyber Security Act

2.13 | Submissions

Deliverable:	2.13
Category:	Submissions
Owner:	Cyber Resilience SIG
Status:	Shipped
License:	CC-BY-SA 4.0
Date:	June 2026

SIG: Cyber Resilience SIG Document type: Submission Number: "2.13" Status: Shipped Editors: Juan Rico Group: European Commission Date: 2026-03-31 Deadline: 2026-05-11 *Find the text submitted below and also attached here*

The ORC Working Group welcomes the opportunity to contribute to the revision of the EU Cybersecurity Act (CSA). We support the EU's efforts to strengthen cybersecurity resilience, trust, and harmonisation across the Single Market. At the same time, we believe the current draft would benefit from greater legal clarity, improved interoperability with the Cyber Resilience Act (CRA), and a more proportionate, risk-based, and innovation-friendly approach to certification and conformity assessment.

The recommendations below focus on ensuring that the CSA remains technically realistic, internationally interoperable, and aligned with modern software development and certification practices.

ORC CSA text analysis

1. Mandatory Security Impact Assessments

- **Analysis (Key Issues):** To ensure a coherent EU cybersecurity framework and avoid undue compliance burdens, new legislation must be assessed for cyber risks from the outset through independent evaluations.
- **Proposal (Recommended Action):** ENISA should conduct mandatory, independent cybersecurity impact assessments for all relevant new EU legislation and its enforcement. These must follow transparent methodologies and be subject to periodic reviews to ensure credibility and oversight. This should complement existing Commission impact assessment procedures while ensuring that cybersecurity-specific risks and implementation impacts are systematically evaluated.

2. Separation of Standardisation Roles

- **Analysis (Key Issues):** A conflict of interest arises if ENISA both drafts contributions to standards and subsequently assesses those same harmonised standards. This risks duplicating work and weakening stakeholder balance.
- **Proposal (Recommended Action):** The legal text must unequivocally reflect Recital 41: ENISA must not help draft standards it is later responsible for assessing. This separation between legislation/standards making and conformity assessment must be operationalised in governance structures. Such safeguards should preserve ENISA's technical expertise and advisory role while ensuring functional independence in assessment and certification activities.

3. Contribution to the Long-Term Sustainability of the CVE System

- **Analysis (Key Issues):** The CVE system is the "universal ledger" of digital risk and the fundamental infrastructure for regulatory compliance, automated defense, and supply chain trust.
- **Proposal (Recommended Action):** ENISA should systematically support the global CVE system through funding bug bounties and investing in vulnerability discovery. This includes structured support for open source maintainers and upstream projects critical to the supply chain. This could include grant-based support mechanisms, coordination initiatives, and long-term funding instruments for critical open source infrastructure maintainers.

4. Transparency of Technical Specifications

- **Analysis (Key Issues):** Relying on restricted or non-public technical specifications for mandatory certification undermines legal certainty and effective market participation.
- **Proposal (Recommended Action):** Technical specifications underpinning certification schemes should be publicly available by default. Any restricted access must be clearly justified, and sufficient information must be provided free of charge to ensure effective implementation. Particular attention should be given to accessibility for SMEs and open source developers that may lack the resources to access proprietary standardisation material.

5. Verification Expectations for Higher Assurance Levels

- **Analysis (Key Issues):** Requiring exhaustive verification of every security-relevant property in technical documentation (per Recital 103) would be disproportionately costly and complex for modern, frequently updated systems.
- **Proposal (Recommended Action):** Clarify Recital 103 to ensure verification requirements remain proportionate and risk-based. This is particularly important for continuously updated systems operating under modern DevSecOps and lifecycle-based development models. The framework should explicitly avoid suggesting that exhaustive verification is mandatory for all described properties.

6. Transitional Provisions (Grandfathering)

- **Analysis (Key Issues):** Protecting past vendor investments requires a "grandfathering" approach to avoid regulatory cliff-edge effects during the transition from national to European schemes.
- **Proposal (Recommended Action):** Existing national certificates should remain valid until their expiry date. The phase-out of national schemes should be linked to clear timelines in Article 86(1) based on the maturity and availability of European alternatives. A phased and predictable transition process is necessary to avoid disruption for both vendors and certification authorities.

7. Flexibility in Mitigation Measures

- **Analysis (Key Issues):** Rigid, "one-size-fits-all" mitigation measures fail to account for different technical architectures and may create unintended operational risks.
- **Proposal (Recommended Action):** Amend Article 103(2) to ensure that while authorities may require mitigation measures, the choice of the *exact* measures implemented remains with the entity, recognising their specific operational context. This approach would preserve technology neutrality while ensuring accountability through outcome-based security objectives.

8. Legal Certainty for Non-Commercial Open Source Actors

- **Analysis (Key Issues):** Ambiguity regarding "placing a product on the market" risks holding non-commercial open-source developers liable, which would discourage community contributions.
- **Proposal (Recommended Action):** Introduce a provision stating that certification and conformity obligations apply exclusively to economic operators acting in a commercial capacity. Explicitly exempt open-source developers acting outside commercial activity from such liability. Clarifying this distinction is essential to preserve collaborative open source security maintenance and avoid discouraging voluntary contributions.

9. Reducing Regulatory Burden and Fragmentation

- **Analysis (Key Issues):** High costs and complexity necessitate simplified pathways for SMEs. To avoid isolation, schemes must build on mature international standards (ISO/IEC) rather than creating parallel requirements.
- **Proposal (Recommended Action):** Maintain the voluntary nature of certification and prioritise alignment with international standards. Introduce simplified pathways for SMEs and FOSS models, including a "presumption of conformity" for entities holding equivalent international certifications.

10. Modernising Certification Structure: Lifecycle, Modularity, and Component Reuse

- **Analysis (Key Issues):** Static, system-centric certification models do not align with modern continuous software development or the reality of open-source modularity.
- **Proposal (Recommended Action):** Focus the ECCF on technical integrity and evolve toward a continuous conformity model. Support modular/component-level certification to enable the reuse of assessment results across multiple products.The framework should progressively support continuous monitoring, update-aware certification, and automated conformity attestations.

11. Supply Chain Policy Coherence and Tool Integration

- **Analysis (Key Issues):** Policy must integrate technical tools like SBOMs and VEX to bridge the gap between high-level regulation and real-world implementation.
- **Proposal (Recommended Action):** Certification schemes should recognise and support the use of SBOMs, VEX, and automated attestations. All certification outputs should be machine-readable, interoperable, and accessible to non-experts. Machine-readable compliance outputs would facilitate automation, reduce administrative burden, and improve supply chain transparency.

12. Interoperability between CSA and CRA

- **Analysis (Key Issues):** The current lack of binding mechanisms between voluntary CSA certification and mandatory CRA assessment leads to duplicative audits and increased compliance costs.
- **Proposal (Recommended Action):** Establish an article allowing European cybersecurity certification schemes to demonstrate a presumption of conformity with CRA requirements. Assessment results and technical documentation should be reusable across both procedures. The framework should support harmonised evidence reuse mechanisms to minimise duplicate assessments and administrative overhead.

13. Strategic Open Source Assurance

- **Analysis (Key Issues):** Excluding open source from the CSA/CRA framework risks creating fragmentation and reduced innovation. Strategic integration enables more transparent, scalable, and automated assurance mechanisms.
- **Proposal (Recommended Action):** Encourage the recognition of open-source-based assurance frameworks and promote the use of open standards and tooling. Policies should be designed to avoid creating unintended barriers to open collaboration. Open standards and open source assurance tooling can support transparency, scalability, and long-term European digital resilience.

ORC proposed amendments

In light of the preceding points, the ORC Community puts forward the subsequent amendments to the existing text.

Amendment	Text proposed	Justification
Cybersecurity Impact Assessments	**New Article 7a - Cybersecurity Impact Assessment** 1. The European Union Agency for Cybersecurity shall carry out independent cybersecurity impact assessments for Union legislative acts and implementing measures that are likely to have a significant impact on cybersecurity. 2. Those assessments shall: (a) identify risks; (b) assess coherence; (c) evaluate compliance burdens. 3. Methodologies shall be transparent and publicly available. 4. The Commission shall ensure periodic external evaluation.	Ensures early risk identification, improves coherence, and introduces accountability mechanisms for ENISA.
Separation of Standardisation Roles	ENISA shall not participate in the drafting of standards or technical specifications which it is subsequently responsible for assessing. **New paragraph: The separation shall be ensured through governance arrangements, including internal procedures and functional separation.**	Prevents conflicts of interest and ensures Recital 41 is effectively implemented in practice.
CVE System Sustainability	**New Article 18a - Support to vulnerability management infrastructure** 1. ENISA shall support the long-term sustainability of the Common Vulnerabilities and Exposures. 2. Support includes: (a) vulnerability discovery; (b) support to open source maintainers; (c) international cooperation.	Recognises CVE as critical infrastructure and addresses systemic risks linked to open source dependencies.
Transparency of Technical Specifications	Technical specifications in certification schemes shall be publicly available. **New paragraph: Where full publication is not possible, sufficient information shall be made available free of charge.**	Ensures legal certainty and usability while accommodating justified restrictions.
Proportionate Verification Requirements	Verification requirements under certification schemes shall be proportionate and risk-based, taking into account assurance level, system complexity, and update frequency.	Avoids excessive burden and ensures feasibility, especially for complex systems.
Transitional Provisions (Grandfathering)	Certificates issued under national schemes shall remain valid until expiry. **New paragraph: Phase-out shall depend on availability and maturity of EU schemes.**	Prevents disruption and ensures realistic transition based on market readiness.
Flexibility in Mitigation Measures	Member States and the Commission may require mitigation measures. **Addition: Economic operators retain discretion over implementation based on risk profile and architecture.**	Avoids rigid, one-size-fits-all obligations and ensures technical feasibility.

Amendment	Text proposed	Justification
Open Source and Liability	**New Article 24a - Scope of obligations** 1. Obligations apply only to economic operators placing products on the market. 2. Non-commercial open source contributors are excluded. **Addition: Responsibilities across the supply chain shall be clearly defined.**	Protects open source ecosystem and clarifies liability distribution.
Reducing Regulatory Burden	Certification schemes shall remain voluntary and build on international standards (e.g. ISO/IEC). **Addition: Provide presumption of conformity or reduced scope for equivalent certifications.**	Reduces duplication, cost, and supports global interoperability.
Continuous & Modular Certification	Certification schemes shall support lifecycle-based and modular approaches. **Addition: Implementation shall be proportionate and phased.**	Aligns certification with modern development while ensuring feasibility.
Supply Chain Tool Integration	Certification schemes shall support SBOMs, VEX, and machine-readable attestations. **Addition: Outputs shall be interoperable and accessible to stakeholders.**	Ensures practical usability and bridges policy with implementation.
CSA-CRA Interoperability	Certification schemes may provide presumption of conformity with the Cyber Resilience Act. **Addition: Results shall be reusable to minimise duplication.**	Reduces compliance costs and avoids duplicate assessments.
Strategic Open Source Integration	Certification schemes shall support open source-based assurance and open standards. **Addition: Measures shall not create barriers to open collaboration.**	Supports innovation, scalability, and alignment with EU digital strategy.

About the ORC Working Group The Open Regulatory Compliance Working Group (ORC WG) brings together open source foundations, global enterprises, and industry stakeholders to address the growing impact of software regulations on open source. With more than 60 members, ORC develops best practices, specifications, and practical resources to help organisations navigate evolving regulatory requirements.