Alliance for AI, IoT and Edge Continuum Innovation

Brussels, 13 April 2026

AIOTI Views on the Cyber Resilience Act

Introduction

AIOTI welcomes the move to regulate for greater cybersecurity. Our members are committed to providing security in our products, we welcome steps to create maximum trust among users and consumers of the safety, security, and resilience of their digital products.

Scope

Effective legislation works best when it focusses on those issues which are critical to achieving the desired outcome. The key question should be 'what are the key practices which we must change to reach our objectives'. In this way efforts can be focussed on areas where we can make most difference without unduly burdening an unnecessarily wide range of other stakeholders. The contributions and comments below are intended to explore areas where greater precision in the regulations might result in more effective regulation.

Limitations and Open Issues

The Regulation places significant emphasis on procedural and documentation requirements, including conformity assessment, technical documentation, and post-market obligations.

There is a risk that a disproportionate focus on formal compliance may divert resources, Cybersecurity risks frequently emerge at the level of system integration, configuration, and operational context rather than from individual components in isolation.

More broadly, the cumulative regulatory impact of the CRA should be considered in the context of the Union's competitiveness and innovation capacity. The interaction of the CRA with other horizontal and sector-specific frameworks may increase regulatory complexity and impose significant compliance burdens, particularly for small and medium-sized enterprises and actors operating across multiple jurisdictions

On the other hand, CRA clarifies key concepts and obligations relating to risk assessment, secure development, vulnerability management, and post-market surveillance, while emphasising the importance of flexibility and outcome-oriented implementation.

This document does not introduce new legal obligations and cannot resolve all underlying ambiguities in the Regulation.

Non-binding nature: As it remains advisory, uncertainties may persist, particularly for borderline products or novel business models, until further delegated acts or enforcement practice emerge.

Complexity for SMEs: While intended to assist smaller enterprises, the sheer breadth of topics and technical detail may still pose a compliance challenge, absent more tailored tools or checklists.

Cloud and SaaS nuances: Guidance on remote and third-party cloud dependencies provides principles but may not yet fully resolve liability or classification risks in highly modular cloud ecosystems.

Contribution on harmonized standards

Harmonized standards are the answer to the new work item concerning products and product components with digital elements that have the basic functionality of identity management and/or privileged access management. Hafenstrom contributes towards line 16 of the standardization request to European Standards Organizations in support of EU policy on cybersecurity requirements for products with digital elements.

Harmonized European Standards cover:

1. General description of the Product with digital elements belonging to that category and the product and/or components such Product with digital elements
2. Description of their use case
3. Security Analysis
4. Definition of applicable risk profiles to be considered for these Product with digital elements
5. Applicable cybersecurity requirements e for each risk profile
6. Applicable cybersecurity assessment and test requirements for each risk profile

Normative references are:

7. prEN 40000-1-1 (on-going Enquiry), Cybersecurity requirements for products with digital elements - Vocabulary
8. prEN 40000-1-2:2025, Cybersecurity requirements for products with digital elements, Principles for cyber resilience
9. prEN 40000-1-3:2026, Cybersecurity requirements for products with digital elements, Vulnerability handling

Identity management systems are hardware and software products with digital elements that provide identity lifecycle management mechanisms, such as identity provisioning, maintenance, authentication, authorisation and deprovisioning, and include associated metadata. Privileged access management hardware and software are products with digital elements that authenticate and authorise users or devices, granting or denying access to digital resources or physical locations. These products (hardware, software and communication protocols) include, but are not limited to, authentication and access control readers, biometric readers, single sign-on software, federated identity management software, corporate/institution/essential entities building protection and multi-factor authentication software.

The purpose is to provide the cybersecurity requirements and the associated conformity assessment of Product with digital elements for a given Intended purpose and for a given security profile based on Common Criteria ISO/IEC 15408 series and ISO/IEC 18045. Our experts have joined the international standardisation of ISO/IEC JTC 1/SC 27/ WG3 since the start in 1990 contributed on smartcard evaluation mechanism Evaluation Assurance Levels (EAL). We also participate actively in CEN TC 224/WG17.

Conclusion

The draft guidance represents the most detailed interpretative resource to date for CRA implementation. It meaningfully clarifies scoping and modification thresholds with structured frameworks and concrete examples, aiding both regulators and companies in preparing for enforcement.

However, as a nonbinding interpretative document, it stops short of settling key legal uncertainties particularly around cloud dependencies, interactions with other EU frameworks, and subjective thresholds such as vulnerability reporting timelines.

In practice, businesses still need robust compliance governance, legal analysis and active engagement in the consultation to mitigate lingering ambiguities before full CRA application dates in 2026–2027.

About AIOTI

AIOTI is the multi-stakeholder platform for stimulating AI, IoT and Edge Continuum Innovation in Europe, bringing together small and large companies, academia, researchers, policy makers, end-users and representatives of society in an end-to-end approach. We strive to leverage, share and promote best practices in the AI, IoT and Edge Continuum ecosystems, be a one-stop point of information to our members while proactively addressing key issues and roadblocks for economic growth, acceptance and adoption of the AI, IoT and Edge Continuum Innovation in society. AIOTI contributions goes beyond technology and addresses horizontal elements across application domains, such as matchmaking and stimulating cooperation by creating joint research roadmaps, defining policies and driving convergence of standards and interoperability.