Warsaw, March 6th 2026

# IS Consulting Position on the Proposed Reform of the Cybersecurity Act (CSA2)

IS Consulting welcomes the European Commission's initiative to revise the Cybersecurity Act and further strengthen the European cybersecurity governance framework. The proposed reform, including the reinforcement of ENISA's mandate, improvements to the European Cybersecurity Certification Framework and the introduction of a more coherent approach to ICT supply chain security, represents an important step toward improving the resilience and competitiveness of the European digital economy.

At the same time, the design and implementation of the revised framework must reflect the structural characteristics of the European economy. Micro, small and medium sized enterprises represent approximately 99 percent of all businesses in the European Union, employ around 100 million people, and generate more than half of the EU's economic value added. As a result, the effectiveness of European cybersecurity regulation will depend largely on its practical applicability for SMEs, which typically operate with limited financial resources, smaller security teams and reduced regulatory capacity.

For this reason, cybersecurity legislation should be designed not only to establish security objectives but also to ensure that these objectives can be implemented effectively across organizations of different sizes and maturity levels. A regulatory framework that is too complex or resource intensive risks limiting adoption and may unintentionally widen the cybersecurity gap between large enterprises and the majority of the European market.

IS Consulting therefore recommends that the CSA reform should be guided by the following policy principles:

## 1. Proportionality and risk based implementation

Cybersecurity requirements, certification schemes and potential cyber posture mechanisms should be designed with proportionality as a core principle. Implementation models should allow phased adoption and differentiated approaches reflecting the risk profile, operational capacity and maturity of organizations, particularly SMEs.

## 2. Certification as a compliance enabling mechanism

European cybersecurity certification frameworks should primarily function as tools that facilitate compliance with EU cybersecurity legislation. Certification mechanisms should help organizations demonstrate alignment with regulatory requirements in a clear and predictable way without creating additional layers of administrative burden.

## 3. Coherence across the EU cybersecurity regulatory framework

The revised Cybersecurity Act should maintain strong alignment with other European legislative instruments, including the NIS2 Directive, the Cyber Resilience Act and sector specific frameworks. Greater interoperability between regulatory instruments will help reduce duplication of obligations and simplify compliance for organizations operating across multiple regulatory environments.

## 4. Technology neutrality and fair competition

Cybersecurity requirements should remain technology neutral and vendor agnostic. Regulatory provisions should focus on functional security objectives and measurable outcomes rather than prescribing specific technologies or vendors. This approach supports innovation, preserves market competition and enables organizations to adopt security solutions appropriate to their operational environment.

## Conclusion

The proposed reform of the Cybersecurity Act provides an important opportunity to strengthen cybersecurity coordination across the European Union and improve the effectiveness of the existing regulatory framework. Ensuring that the framework remains proportionate, operationally feasible and aligned with the SME driven structure of the European economy will be essential for achieving broad adoption of cybersecurity practices and improving the overall resilience of the European digital ecosystem.