Warsaw, March 23rd 2026

Statement on the ENISA Ad Hoc Working Group on Cybersecurity Standardization

IS Consulting welcomes the establishment of the ENISA Ad Hoc Working Group on Cybersecurity Standardization and recognizes the importance of this work for the future coherence of the European cybersecurity framework. ENISA's terms of reference correctly position the group as a mechanism to support the identification and mapping of relevant standardization initiatives, the review of gaps and overlaps, the monitoring of international developments, and the creation of synergies across existing initiatives while avoiding duplication. This direction is consistent with ENISA's wider mandate to facilitate the uptake of European and international standards and with our own public policy principles, which emphasize operational feasibility, proportionality, transparency, vendor neutral requirements and fair competition, with particular regard to the realities of micro, small and medium sized enterprises.

At the same time, the practical legitimacy of any standardization effort depends not only on its formal mandate, but also on the balance of perspectives reflected in its working structures. ENISA states that the group should pursue broad, interdisciplinary representation and an appropriate balance across stakeholder communities. Based on the announced membership, however, the current composition appears weighted towards large technology providers, trust service actors, conformity assessment bodies and other established corporate stakeholders, while the voice of organizations focused on practical SME implementation appears comparatively limited. That imbalance matters, because standardization choices that are technically coherent in large enterprise environments may prove difficult, costly, or unrealistic when translated into the operating conditions of smaller businesses.

This concern is not peripheral to the European economy. SMEs represent 99% of all businesses in the European Union. The European Commission has also stated that SMEs provide two thirds of private sector jobs in the EU and account for more than half of value added in the non-financial business

sector. Any standardization approach that does not adequately reflect SME implementation capacity therefore risks being disconnected from the economic structure it is ultimately meant to serve.

From the perspective set out in our public policy framework, the core policy risk is twofold. First, Europe too often tends to create new regulatory or quasi regulatory layers where credible international or market standards already exist and could instead be recognized, mapped, profiled or made interoperable. Second, requirements are frequently framed around an enterprise class governance and assurance model, assuming dedicated cybersecurity teams, mature procurement functions, formalized third party assurance, continuous documentation and evidence production, and the capacity to absorb recurring compliance overhead. For many SMEs, these assumptions do not reflect operational reality. The result is not stronger resilience, but a widening gap between formal compliance architecture and practical adoption capacity. ENISA's own terms of reference, including the explicit reference to alignment with international standards and existing industry best practices, point in the right direction and should remain central to the group's work.

A standard that is not implementable at scale across the SME economy will not deliver broad European resilience. In practice, the main risks for SMEs are clear: excessive abstraction, excessive evidence burdens, fragmentation across overlapping frameworks, implicit preferences for enterprise oriented technologies and service models, and assurance expectations that are disproportionate to size and risk. Our public policy position is that cybersecurity requirements should be risk based, operationally feasible and staged, with a clear minimum baseline and realistic maturity pathways, rather than designed around the capabilities of the largest organizations and then imposed downward on the rest of the market.

For that reason, IS Consulting encourages ENISA and the members of the Ad Hoc Working Group to apply five principles throughout their work. First, preference should be given to alignment with existing international and market standards where these are already fit for purpose. Second, baseline controls for broad market adoption should be clearly distinguished from advanced measures intended for high criticality or high complexity environments. Third, evidence and assurance expectations should be proportionate to organizational size, sector, and risk exposure. Fourth, recommendations should remain vendor neutral and avoid embedding

assumptions that indirectly privilege enterprise architectures over more accessible implementation models. Fifth, draft outputs should be tested against real SME implementation scenarios before they are stabilized as reference points for wider European use. These principles are fully consistent with our public policy commitment to feasibility for SMEs, proportionality, functional requirements, and fair competition.

Europe's cybersecurity resilience will not be strengthened by designing standards primarily for the most resourced organizations and expecting the rest of the economy to adapt at their own expense. It will be strengthened by building a framework that is technically credible, internationally aligned, economically realistic and deployable across the full breadth of the European market. In that respect, the contribution of SME oriented implementation perspectives is not a secondary consideration. It is a condition for effective standardization..