# Digital Omnibus

## Forvis Mazars Response to the Call for Evidence

**14 October 2025**

Forvis Mazars is a global firm born in the European Union: we deliver audit & assurance, tax, advisory and consulting services in 26 Member States and over 100 countries and territories. As a professional services firm that assists clients with implementing digital and IT regulations and requirements related to AI systems and cyber security challenges, we welcome the opportunity to provide evidence to support the smooth application of the AI Act rules, the Apply AI strategy, including by ensuring the optimal application of the Artificial Intelligence Act, and the initiative to revise the Cybersecurity regulatory framework.

As a leading professional services firm with deep expertise in cybersecurity, risk management, and regulatory compliance across the European Union, we are committed to supporting the development of robust, harmonised AI and cyber risk frameworks. Our response draws upon practical experience advising public and private sector organisations on cyber resilience, and governance (including the provision of third-party cyber security assurance), and reflects our dedication to safeguarding the digital ecosystem.

# AI Act

## (I) Optimal Application of the Rules – Risk Based Approach

The call for evidence emphasises that the optimal application of AI rules under the Digital Omnibus should make compliance practical and effective without undermining the objectives of the AI Act. This means aligning obligations with real-world implementation challenges and ensuring businesses, especially SMEs and mid-caps, can comply without disproportionate costs. The AI Act's risk-based approach is critical, however, clear operationalisation criteria for the Act risk classification are not always clear.

While it is understood that obligations should scale with the potential impact of an AI system, focusing stringent requirements on high-risk applications (e.g., medical diagnostics, recruitment algorithms) while simplifying processes for low-risk tools like chatbots or internal analytics, clear and actionable guidelines are essential to operationalise this principle. For example, decision trees and sector-specific examples helping classify risk levels, along with templates for conformity assessments and post-market monitoring should be provided and can act as guidelines on how to apply the requirements of the Act. Without such clarity, companies often struggle.

For example, a mid-sized HR tech firm deploying AI for candidate screening may not be clear as to whether its system qualifies as "high-risk," leading to costly over-compliance. Similarly, a healthcare startup could face delays where it lacks guidance on the harmonisation of the AI Act obligations with GDPR and other laws. These examples illustrate why proportionality, clear, and harmonised standards should underpin any implementation whereby reducing any ambiguity while safeguarding rights and safety.

To ensure the optimal application of the AI Act, a clarification of risk classification criteria, including the operationalisation of the principle of AI impact, as well as enabling proportional compliance for smaller firms is essential to avoid over-compliance and stifling innovation.

### (II) Legal Predictability

The optimal application of AI rules should be accompanied by a high degree of legal predictability, enabling organisations to plan, develop and invest with certainty and confidence. Legal predictability requires clear, stable, and harmonised interpretations of obligations across all Member States, avoiding fragmented enforcement that generates uncertainty and compliance risk.

For example, an automotive manufacturer deploying AI for autonomous driving and a retail company implementing AI-driven dynamic pricing are both classified as high-risk under the AI Act, however, their regulatory contexts differ substantially. Autonomous driving intersects with vehicle safety and liability frameworks, while dynamic pricing raises concerns under consumer protection and competition law. Without consistent guidance, these organisations can incur excessive compliance costs or delay implementation due to fear of conflicting interpretations. To address this, the Commission should publish sector-specific compliance roadmaps, decision trees for overlapping frameworks, and implementation timelines aligned with enforcement readiness. Harmonisation with established standards (such as ISO/IEC 42001), integration with GDPR and the Cybersecurity Act, and the creation of a centralised EU guidance portal would help reduce ambiguity.

Legal predictability is a fundamental prerequisite for innovation and competitiveness in Europe's digital economy.

## Cyber Security

Our contribution is focused on four main issues:

- Clarifying the Mandate of ENISA
- Positioning third party assurance within the broader EU legal framework
- Improving the European Cybersecurity Certification Framework
- Achieving Better Resilience

### (I) Clarifying the Mandate of ENISA

Clarity regarding the mandate of the EU Agency for Cybersecurity (ENISA) is essential for effective governance and coordination. We recommend that the revised Act explicitly define ENISA's scope, roles, and responsibilities as follows:

- Strategic Leadership: ENISA should be empowered to set strategic priorities and provide authoritative guidance on cybersecurity matters, supporting both national agencies and EU institutions.
- Operational Coordination: ENISA's mandate should encompass the facilitation of cross-border incident response, intelligence sharing, and crisis management, ensuring coherent action during major cyber events.
- Capacity Building: ENISA should lead efforts in training, awareness, and skills development to address the growing talent gap and promote a culture of resilience.
- Stakeholder Engagement: The Agency should act as a central point for stakeholder consultation, facilitating dialogue between regulators, industry, academia, and civil society.

A clear and robust mandate will enable ENISA to fulfil its mission effectively and support the EU's cybersecurity objectives.

## (II) Specific Recommendations for Auditing Cybersecurity Compliance

We recognise that whilst the recent adoption of cyber security directives such as NIS2, DORA and the Cyber Resilience Act are improving the EU's cyber resilience, they have resulted in overlapping obligations and some divergences in their application at Member State level, not all of whom have yet enacted the directive. This is leading to an imbalance in cyber resilience between Member States and an inconsistency in approaches to supervision and enforcement, with many national regulators struggling to cover their significantly increased mandates.

We recommend the following

- Mandating Regular Independent Audits: Organisations covered by the obligations should be required to undergo regular, independent cybersecurity audits by third party auditors. These audits should assess compliance with EU cyber security obligations, identify gaps and make recommendations for improvement.
- Standardising Audit Methodologies: The EU should develop and promote standardised audit methodologies and reporting frameworks to ensure consistent assessment and comparability of results across Member States. This could include sector-specific guidelines and risk-based approaches tailored to organisational size and type.
- Centralised Oversight: ENISA should coordinate or oversee a centralised registry of audit firms
- Integration with Incident Reporting: Audit findings should be linked to incident reporting mechanisms, ensuring that recurring weaknesses identified through audits are addressed as part of broader risk management and response planning. Incident reporting obligations should be proportionate and designed to minimise administrative cost.

These recommendations aim to enhance transparency, accountability, and continuous improvement in cybersecurity compliance across the EU.

## (III) Improving the European Cybersecurity Certification Framework

The European Cybersecurity Certification Framework is a cornerstone for enhancing trust and security in digital products and services. To further improve its efficiency, inclusivity, and adaptability, we propose the following recommendations:

- Streamlining Processes: Simplifying certification procedures to reduce administrative burdens and accelerate time-to-market for innovative solutions, especially for SMEs.
- Inclusive Standards Development: Ensure that certification schemes are developed through transparent, multi-stakeholder processes, incorporating feedback from industry, users, and technical experts.
- Adaptive Schemes: Introduce mechanisms for regular review and updating of certification criteria, allowing frameworks to evolve alongside technological advancements and emerging threats.
- Mutual Recognition: Promote interoperability and mutual recognition of certificates across Member States to foster a harmonised single market for cyber security products and services.

These improvements will enhance the framework's relevance, accessibility, and effectiveness, ultimately contributing to a safer digital environment for all.

## (IV) Achieving Better Resilience

Resilience must be at the heart of the revised Cybersecurity Act. We advocate for the following measures to strengthen the EU's cyber posture:

- Harmonisation: Encourage alignment of cyber security requirements and practices across Member States to minimise fragmentation and facilitate coordinated responses. Harmonisation of requirements and compliance processes as well as providing clear reciprocity where compliance with one regulation qualifies as compliance with other regulations would support both the objective of simplification and also ensure greater compliance levels by businesses who are more likely to allocate resources to a suite of harmonised requirements that multiple disparate requirements
- Capacity Building: Invest in education, training, and resource development to build a skilled workforce and promote continuous improvement in cyber defence.
- Continuous Improvement: Establish feedback loops and monitoring mechanisms to assess the effectiveness of cyber security measures and inform future policy and regulatory updates.

By prioritising resilience, the EU can better withstand and recover from cyber incidents, protecting citizens, businesses, and critical infrastructure.