Christina Papaconstantinou: Implementation status of key regulations – DORA, MiCAR, Basel IV, Genius Act and the AI Act – and what early enforcement reveals

Speech by Ms Christina Papaconstantinou, Deputy Governor of the Bank of Greece, at the World Banking Forum, Athens, 30 October 2025.

* * *

Good morning,

I would like to thank you for inviting me to the World Banking Forum to speak today about the implementation status of key regulatory texts and the lessons learnt from their enforcement so far.

This address comes at a moment when stakeholders, including policymakers, call strongly for "simplification" and the "easing" of regulatory burden. At the same time, "de-regulation" is being brought up in this discussion more often now than, probably, ever before. In fact, what financial institutions really need the most, in this era of significant digital transformation, economic uncertainty and geopolitical tensions, is **stability** and **convergence**.

For this reason, regulatory texts – such as the ones I will talk about today – that bring legal certainty, ensure a level playing field across the EU and aim to manage risks while promoting innovation are of paramount importance.

I will first start with the Digital Operational Resilience Act or DORA:

DORA

As finance becomes overwhelmingly digital, institutions that harness new technologies gain a competitive edge by providing consumers with round-the-clock access to their systems and instant transaction times. A significant number of financial institutions rely on technologies like cloud infrastructure, apply data-driven processes and utilise AI capabilities to deliver services faster and more effectively. What sets the current digital transformation apart from others that took place in the past is its **pervasiveness,** with dense interconnections and interdependencies across countries, firms, markets and third-party providers of ICT services. Yet, the same interdependence that enables competitiveness gains also **amplifies operational and cyber risks**, including concentration in critical ICT service providers and more complex incident cascades.

This is precisely why **DORA matters**: for the first time, we have a single, technology-neutral framework on digital operational resilience across the financial sector, aimed at safeguarding the transition from traditional models to the digital age. DORA consolidates and strengthens those ICT risk management requirements that up until now were spread over various financial services legislative texts, giving us a stable operational backbone on which financial digital innovation can thrive more safely.

But what does DORA actually change for financial institutions? Beyond consolidating familiar expectations on ICT risk, DORA introduces, among other things, three innovative solutions to major areas of concern. **First, common major incident reporting,** meaning single EU taxonomy, timelines and data standards for major ICT incidents and significant cyber threats, which enable their comparability, along with faster and more coordinated action to address them. **Second, mandatory threat-led penetration testing (TLPT):** this means that, for selected entities and on a 3-year cycle, control-checklists are replaced by intelligence-led, scenario-based tests that validate real-world operational resilience. **Third, direct EU-level oversight of critical ICT third-party providers (CTPPs):** this recognises concentration and contagion risks in shared infrastructures.

These innovations introduced by DORA, when combined with strategy, governance and testing obligations, shift operational resilience from being just an "IT topic" to an enterprise-wide capability, which requires clear understanding and sufficient support by senior management.

Ten months into the implementation of DORA in January 2025, we can safely discuss some early conclusions from its enforcement so far. Our first observation is divergence in the **institutions' maturity levels:** as expected, credit institutions are typically ahead, reflecting their adherence to earlier ICT-risk regulatory regimes. On the other hand, insurers, payments and e-money firms and the newly included in our supervisory perimeter IORPs [Institutions for Occupational Retirement Provision] are moving fast, but from a lower starting point compared to credit institutions, towards meeting DORA expectations.

Another observation **is uneven operational mapping.** Some financial entities still struggle to map critical or important functions against accountable owners, supporting processes, information assets and ICT services and, moreover, to keep those maps and asset inventories up to date as their systems and architectures evolve. Since DORA's perimeter is the entire organisation, from data lineage to customer-facing processes, rather than just networks and servers, it takes time and disciplined and documented steps to understand how to identify the critical or important functions and map them in relation to the rest of the digital ecosystem.

As expected, **ICT third-party risk management** is currently the heaviest lift. In Greece, our points of attention for financial entities are consistent with those in the rest of the EU: build a high-quality error-free Register of Information; institute a third-party management system that detects underachieving service level agreements and concentration risks; and adopt a durable contract-review methodology to include rights to audit and test, visible sub-outsourcing, meaningful exit strategies and data-portability clauses that can be applied at scale across hundreds of arrangements.

Furthermore, according to our data, **major incident management** still needs sharper reactions, clearer thresholds for what constitutes a "major incident", faster internal escalation, disciplined external notifications and better stakeholder communications when events are unfolding.

Resilience testing must also mature from ad-hoc penetration tests to risk-based annual programmes; this requires building up the internal coordination capacity (to scope, manage purple-team exercises and govern remediation) and securing credible threat-intelligence and testing partners.

Finally, **strategy and governance** also come to the fore with the requirement for a firm-wide **digital operational resilience strategy.** This strategy, which should include scenario testing, investment roadmaps and regular board engagement, should expose gaps in the management of ICT risk and be linked to a periodic review of the ICT risk-management framework.

Beyond our observations at local level, early feedback from DORA policy work at EU level **has underscored the need for stability and clarity.** Stakeholders asked for proportionality, streamlined incident criteria and consistent treatment of subcontracting and outsourcing. On paper, this has been achieved with the adoption of standards; however, **consistent application among supervisory authorities remains the real test** and this is why **further supervisory convergence** in key areas is imperative.

Turning now to MiCAR:

MiCAR

In the EU, markets in crypto-assets are regulated by the provisions of the Regulation [(EU) 2023/1114] widely known as **MiCAR**, which became fully applicable on 30 December 2024. MiCAR is designed to protect investors and safeguard market integrity, while at the same time addressing systemic risks linked to crypto-assets that purport to maintain a stable value. These risks concern financial stability, payment systems, monetary policy transmission and monetary sovereignty. Importantly, MiCAR leverages the development of crypto-assets to support innovation in the sector. At EU level, supervisory convergence is fostered by the EBA and ESMA, in close collaboration with national supervisory authorities.

In **Greece**, the 2025 Law [5193/2025] on the Enhancement of the Capital Market establishes the national measures for the implementation of MiCAR, assigning respective competences and powers to the Hellenic Capital Market Commission and the Bank of Greece. The Bank of Greece has been entrusted with the prudential supervision of credit institutions, electronic money institutions and payment institutions that plan to issue e-money tokens (EMTs) and/or asset-referenced tokens (ARTs) or to operate as crypto-asset service providers (CASPs). It is also empowered to license these entities and to impose administrative measures or penalties for breaches of the Regulation.

Recent developments show that the stablecoin market has grown rapidly, increasing its linkages with the financial sector and thereby creating potential implications for euro area financial stability, banking sector soundness, payment systems and the international role of the euro. US dollar-denominated stablecoins dominate the global market, while euro-denominated stablecoins remain marginal. Nevertheless, growth in the latter has picked up since early 2025 following the regulatory clarity provided under MiCAR. Market concentration also appears to be high.

Two key **concerns** have emerged in connection with the implementation of MiCAR. **The first** relates to **multi-issuance schemes**, meaning fully fungible stablecoins issued jointly by EU and third-country entities. As noted recently by the ESRB, such schemes have built-in vulnerabilities and may operate under regulatory regimes which are much more lenient than those for financial conglomerates, raising the question of divergent prudential standards. **The second concern** relates to the **interplay between MiCAR and the revised Payment Services Directive (or PSD2)**, particularly for e-money tokens, where certain activities could trigger overlapping requirements under both regimes. This gives rise to a risk of double licensing and regulatory complexity, which supervisors and the EBA are seeking to address through transitional arrangements and future alignment of the two frameworks.

At the global level, the regulatory landscape remains fragmented, creating risks of regulatory arbitrage and cross-border contagion. In the United States, the **Genius Act** advances federal stablecoin legislation, but with a **narrower scope than MiCAR**, covering only payment stablecoins. Its provisions are generally **more favourable to the development of stablecoins**, including broader eligibility of reserve assets, exemptions from certain capital requirements and the possibility for service providers to pay interest, which MiCAR prohibits. Such divergences may give US issuers a competitive edge, reinforcing the dominance of US dollar-denominated stablecoins.

To safeguard European interests, it will be essential to close interpretation gaps in MiCAR, promote euro-denominated alternatives, accelerate progress towards the digital euro and develop DLT-based settlement solutions. Identifying potential future adjustments to MiCAR will also be key to ensuring a level playing field with issuers in other jurisdictions while effectively managing risks.

Regarding the AI Act:

AI Act

The Artificial Intelligence Act, enacted via an EU Regulation in 2024 [(Regulation (EU) 2024/1689)], establishes the world's first comprehensive regulatory framework for artificial intelligence. It will become fully applicable in August 2026, while certain obligations, such as prohibiting AI systems that are deemed to carry unacceptable risk, have already taken effect. The AI Act seeks to balance the **protection of fundamental rights with the promotion of innovation in AI**. The most important AI Act obligations relate to the management of potential risks before an AI tool is put into productive operation; transparency in order to ensure that natural persons are always aware if they are interacting with AI systems and that content generated or manipulated by AI systems is flagged as such; as well as safety and accuracy. Obligations are addressed to all entities in the value chain.

The AI Act applies a risk-based approach, distinguishing between:

- Prohibited AI practices, such as social scoring by public authorities.

- High-risk systems, subject to strict obligations relating to risk management, data governance, human oversight, transparency and post-market monitoring.

- Limited-risk systems, such as chatbots, subject to transparency obligations.

The AI Act has established **several bodies and fora at the EU level** to coordinate enforcement, ensure consistent implementation and address systemic risks arising from general-purpose AI models.

In Greece, implementation of the AI Act is coordinated by the Ministry of Digital Governance. Preparatory work is underway to identify the competent authorities and establish national governance structures.

Looking ahead, the success of the AI Act will rely on close cooperation among authorities, sufficient technical expertise and a balanced approach that fosters innovation while upholding trust and accountability in the use of AI across critical sectors.

Turning now to Basel IV:

Basel IV

Basel IV standards represent a major evolution in global banking regulation. They are designed to strengthen the resilience and stability of financial institutions; enhance prudential oversight, governance and risk management across the EU banking sector; provide stronger tools for monitoring emerging risks; upgrade stress testing; and improve supervisory reviews.

The reform process related to the Basel standards culminated, after extensive negotiations, in the adoption in 2024 of Regulation [(EU) 2024/1623], commonly known as the Capital Requirements Regulation (or CRR III), and Directive [(EU) 2024/1619], also known as the Capital Requirements Directive (or CRD VI). CRR III has been directly applicable since 1 January 2025, while CRD VI shall be transposed into the Greek law by 10 January 2026.

The implementation of CRD VI will introduce **new rules for both EU and non-EU banks operating in Greece**. Notably, third-country credit institutions that provide core banking services in Greece will be required to apply for authorisation to establish a subsidiary. Moreover, EU banks must notify in advance the Bank of Greece of any mergers or divisions, material transfers of assets or liabilities, acquisitions of material holdings in other entities, and will be subject to periodic penalty payments, on top of administrative penalties and measures, under an enhanced sanctioning regime. These are some of the upcoming changes, under this harmonised set of rules, which, overall, brings more activities under direct supervisory oversight.

I will close my intervention today with a reference to the CMDI framework and the current work on simplification:

The EU Council and the European Parliament have recently reached an agreement on the **Crisis Management and Deposit Insurance (CMDI) framework**. This will mark a significant improvement in the EU framework for managing the failure of banks. The agreed provisions enhance especially the ability of authorities to deal with small and

medium-sized banks that could have implications for financial stability either at national or regional level. They will facilitate access to industry-funded safety nets to finance failing banks' resolution and eventual exit from the market. Banks with insufficient MREL (Minimum Requirement for Own Funds and Eligible Liabilities) capital can, as a last resort, rely on Deposit Guarantee Schemes or resolution funds (or on the Single Resolution Fund in the banking union) to finance their resolution without bailing-in their depositors. To safeguard financial stability and minimise moral hazard, this "bridge the gap" mechanism will be subject to strict safeguards, ensuring that MREL capital remains the primary line of defence.

Given the agreement reached on the CMDI framework and the enhanced resilience of the euro area banking system, it is time to press ahead with the establishment of the **third pillar of the Banking Union**. The EDIS (or European Deposit Insurance Scheme) would strengthen the resilience of the banking sector even further, as it could fully cover both liquidity needs and losses in resolution. A common scheme would ensure that the level of confidence in the safety of bank deposits is equally high across all Member States, thereby reducing the risk of bank runs and safeguarding financial stability. Keeping depositor protection at the national level maintains the bank-sovereign nexus, impedes the creation of a level playing field and weakens financial stability.

As my concluding remark, I would like to note that the EU is currently working on the **simplification** of the EU regulatory framework. This started with the publication of the Draghi Report, and before that the Letta Report, both of which singled out regulatory simplification as key for unlocking EU competitiveness. EU Institutions have initiated efforts to simplify supervisory rules and practices in order to remove unnecessary complexity, enhance coordination and achieve shorter implementation timeframes. *Simplification*, as perhaps you have heard before, does not mean *de-regulation*. Supervision and regulation form a framework that preserves financial stability, protects depositors and shields the real economy from the impact of bank failure. This ***safety net*** **should not be compromised** in any way.

The Bank of Greece fully supports this initiative, stands ready to take on the powers and responsibilities assigned by the regulatory framework and will continue working to maintain stability, facilitate progress and support economic growth.

Thank you.