Martin Moloney

Deputy Secretary General,
Financial Stability Board

Enhancing supervision: challenges and opportunities for the EU

Disclaimer:

The views expressed in these remarks are those of the speaker in his role as FSB Deputy Secretary General and do not necessarily reflect those of the FSB or its members.

I'm told that the last public execution in this lovely city of Copenhagen occurred in the 1770s for a form of securities fraud. In an important sense, all forms of penalty imposed on an entity reflect the reality either that supervision has failed or that it hasn't been tried. A key part of getting closer to 'the system working well' – and a part that, I suggest, is particularly relevant to the EU – is whether supervision and the structure of regulatory institutions is working well. In different parts of the world, pre-emptive supervision and post-fact enforcement play different roles and these are legitimate differences of approach. The European approach, entirely legitimately, places a predominant reliance on supervision; but the organisational structures are, as the IMF observed in its recent Financial Sector Assessment Program on Euro Area policies, complex.

At its heart, supervision relies on two key ideas:

- First, that human beings tend to comply more with rules when there is a chance that their compliance will be checked; but
- Secondly, and perhaps more importantly, that financial service providers want to manage their own risks and will benefit from an external party checking how well they are doing that.

Both goals need to be attended to in good supervisory practice. But you are winning when you are promoting good risk culture and you are in some difficulty when you are forced to focus on checking compliance.

It is important for Europeans to ask themselves: 'Given how complex our supervisory structures have to be, how do we know we are doing supervision well?'

What we all saw in the banking turmoil of 2023 was how supervisory problems can leave you with a crisis on your hands no matter how good the rules. Let me take a now-familiar, non-European example: Silicon Valley Bank was an example of a bank with an unusual business model and very substantial interest rate risk, where the supervisors struggled to compel the management to adopt appropriate risk management practices.

The old saying is that hard cases make bad laws, but they do make for good examples for supervisory training.

To achieve good supervisory outcomes, we must promote among our supervisors a capacity for well-balanced and well-informed judgement. Understanding that leads me to suspect that the FSB will need to do more at a global level on the quality of supervision itself. How should the EU also think about this question of the quality of supervision?

Let me illustrate the particular European challenge with a couple of examples: cyber and crypto.

Cyber resilience

In the case of cyber risk, we all know that we are operating in an increasingly dangerous environment.

The challenges are cross-societal rather than financial sector specific; but they are also cross-jurisdictional, particularly as the EU becomes more integrated. The EU has wisely developed an ambitious piece of legislation in the form of the Digital Operational Resilience Act (DORA).

But challenges remain.

Reliance of the EU financial sector on cross-border, third-party, critical service providers is rising. Small companies understandably struggle with the increasingly burdensome and costly requirements of good security. Within member States, regulatory authorities can be fragmented, applying different approaches or standards to different sectors. Incident notification arrangements can be fragmented, slowing the response speed down.

Comprehensive threat intelligence needs to be gathered in every member State, centralized and distributed out. The initiative of the ECB in developing the Threat Intelligence Based Ethical Red-teaming (TIBER) framework is particularly welcome in that it sets a base level for the quality of testing of the resilience of entities which provide core financial infrastructure in the EU. But

even this welcome standardised approach to testing faces the risk that the criminals can develop more quickly than the EU community can respond. Inadequate testing can become a dangerous reassurance.

Jurisdictions in the EU have an opportunity to develop a unified jurisdictional map of the threat landscape. Information in the DORA registers could provide deeper insights into the changing structure of the sector and the emerging risks. I understand that these registers have a way to go in jurisdictions before this information is comprehensive. But when they are, national analysis of the third-party contracts will provide a rich source of information on concentration risk and channels of systemic risk which should feed into supervisory planning. Getting to that situation is very important precisely because the sector is changing so quickly.

Slow information exchange during an incident can be a major cause of harm. The FSB has done important practical work in developing its Cyber Incident Response toolkit[1] and the Format for Incident Reporting Exchange (FIRE)[2] to promote prompt and efficient responses to attacks. FIRE was developed to tackle fragmented reporting requirements and coordination challenges across jurisdictions. The EU needs consistent, efficient approaches that reduce operational burdens and ensures speedy incident-response communication within and across EU jurisdictions.

Supervisory approaches which engage smaller financial entities to get their defences into as good a state as possible, within the costs they can bear, are needed throughout the EU and will require prudent exercise of judgement by supervisors, rather than a one size fits all approach. Where one sectoral regulator develops good practice, this needs to be shared across the jurisdiction. I cannot over emphasise the importance of a robust schedule of onsite supervisory visits, but done by expert supervisors who understand what good looks like in terms of cyber protections. This is not just about checking that there are cyber risk governance procedures in place, it is about the supervisor providing the senior leadership of a financial services firm with an honest, if sometimes uncomfortable, message about how well prepared they are for a cyber-attack and being listened to when they provide that message. Strong supervisory judgement is required to do that well, but it is costly and difficult to put in place the required expertise.

The EU like many other parts of the world is constantly being eyed by cyber criminals as full of potential rich pickings. Whenever they are successful in the financial sector in the EU, one of the potential reasons for their success might be this complex set of supervisory arrangements under DORA, unless care is taken. I am not saying that the DORA framework is inherently flawed or anything like that. I am saying that its complexity requires – as the ECB recognized with TIBER – that there must be a relentless drive to make this complex system work to a high standard.

The Artificial Intelligence (AI) Act has wisely recognised the cyber risk attaching to AI models. It has imposed on General Purpose Artificial Intelligence Systems, which are systemically risky, requirements for advanced cyber security measures. Supervision sits, again, with national competent authorities, this time with the EU AI Office having a coordinating role. The structure is entirely legitimate. The challenges for the quality of supervision are evident.

Crypto-assets

In its recently published tenth edition of its Nonbank Financial Intermediation Risk Monitor, the European Systemic Risk Board highlighted that the interconnectedness between crypto-assets and traditional finance have intensified at the same time as there has been a sharp rise in crypto-asset valuations and the expansion of stablecoins. They, rightly, emphasised the necessity for comprehensive risk monitoring.

Crypto-assets are an obvious area of emerging risk. This reality demands well-designed regulation and insightful supervisory oversight of these activities.

The EU's Markets in Crypto-Assets Regulation – or MiCA –aims to establish a comprehensive regulatory framework for crypto-assets, particularly the service providers that operate in this space. From our perspective, having made global recommendations on this issue, this is very welcome.

However, the implementation of MiCA is complex. Much of the supervision is delegated to member States. There is still a distance to go in translating MiCA into fully functioning supervisory regimes across all member States.

This degree of delegation also creates coordination challenges for EU and national authorities, who must ensure that the 27 national competent authorities regulate and supervise crypto-asset activities consistently.

Innovation often outpaces regulation. When regulatory frameworks lag, supervision serves as the critical first line of defence to address emerging risks. It must be good enough.

Supervisors must anticipate threats as crypto firms rapidly expand their products and offerings, such as crypto-asset borrowing and lending, which currently falls outside the scope of MiCA. Regulatory updates will, no doubt, close these gaps in time. In the meantime, having supervision so fully distributed across 27 national authorities is a particular EU challenge for holding the line.

It makes sense to delegate the supervision of small innovative entities to member States. But that is a challenge if operating across borders is at the heart of the business model of those small innovators. It becomes even more of a challenge when some of the entities whose regulation is being delegated in this way are not small innovators but large well-established global firms, as is the case in the crypto sphere.

Supervising crypto-asset service providers requires significant resources and expertise. The delegated model that the EU has adopted requires the EU to duplicate expensive supervisory expertise. Ensuring robust supervisory oversight of complex, globally active entities requires a unified approach that transcends national boundaries, leveraging shared expertise and fostering consistent standards. This challenge, however, is not unique to the EU. In the FSB's 2024 crypto progress report, 80% of member jurisdictions identified cross-border coordination and cooperation as a 'very important' regulatory challenge. But the issue of coordination within the EU is both a particular challenge and a particular opportunity because of the regulatory structure issue.

Conclusion

In the end, in my view, supervision should target the supervision of the culture of a firm and the goal of supervision should be to promote effective management by the firm of the risks it faces. Of course, that is not always possible. Incentives can be misaligned, and financial services providers can intentionally break rules. In that case, supervision becomes the handmaiden of enforcement. But ideally, we should never reach that point.

One of the questions we have to ask at the FSB is if there is more we can do to promote good supervision across the globe.

One of the questions, you all face as members of the EU is how to achieve robust high standards of supervision across the EU, while respecting the competencies of member States and the complexities of the structure of the EU itself. One of the choices the EU has to face every time it introduces a new regulatory regime is how to structure the supervisory responsibilities. As such regimes are rolled out, it can become quickly obvious that the chosen structure could be refined for better effect. Where that happens, is the EU able to respond nimbly?

We are moving further and further into a period where sensitivity to the relationship between regulation and growth is rising, and geopolitical uncertainties are morphing endlessly into new threats and challenges. I suspect all European policy makers will increasingly come to the realisation that weak supervision is becoming even more of a core risk and wise supervision is a strategic opportunity. Just yesterday at this very conference, the Commissioner's remarks suggest the opportunity is understood. This is good news. Thank You.

1. https://www.fsb.org/2020/10/effective-practices-for-cyber-incident-response-and-recovery-final-report/.
2. https://www.fsb.org/2025/04/format-for-incident-reporting-exchange-fire-final-report/.