29 May 2026
ESMA91-372-1582

Keynote speech

6th EACH CEO Summit, Paris, 28 May 2026

Klaus Löber
Chair of the ESMA CCP Supervisory Committee

Ladies and gentlemen,

It is a pleasure to be with you again and to engage with those who run CCPs at the very heart of our financial system.

When we met last year, I highlighted the growing relevance of geopolitical risk and the implications for financial market infrastructures. Since then, the environment has become, if anything, even more demanding. Geopolitical tensions remain elevated, volatility can return abruptly, and technological change is moving at a pace that creates both opportunities and new vulnerabilities.

Against this background, ESMA continues to look into the evolving risk landscape for EU CCPs. One of the tools we use is our annual CCP heatmap, which provides a structured and forward-looking view on key risks facing the clearing ecosystem.

The current iteration of the heatmap identifies six priority areas.

First, cyber and operational resilience, including dependencies on cloud and other third-party providers.

Second, market risk, especially in an environment shaped by geopolitical uncertainty and sudden repricing.

Third, procyclicality of margins and collateral, where resilience needs to be preserved without amplifying stress.

Fourth, governance and controls, including the implementation of EMIR 3 and the management of third-party risks.

Fifth, financial innovation, including artificial intelligence, tokenisation, crypto-related developments and other technology-driven changes to market structure.

And sixth, business risk, including profitability, competitive dynamics and capital resilience in a changing market environment.

These risks are increasingly interconnected. Market stress can expose operational weaknesses. Innovation can improve efficiency, but also create new dependencies. Governance weaknesses can amplify vulnerabilities elsewhere. That is why the heatmap is not just a diagnostic tool. It helps guide where supervisory attention needs to deepen.

Today, I would like to focus in particular on operational resilience — especially cyber resilience and third-party risk — before turning to the challenges and implications of AI, cloud, tokenisation and quantum computing.

The state of play: resilience tested by a changing environment

Let me begin with the broader picture. CCPs have, overall, continued to show resilience in a demanding environment. Clearing services have remained robust through episodes of market stress, and CCPs continue to play a central role in supporting orderly and efficient markets.

But resilience should not be confused with being immune. The operating environment is becoming more complex, more interdependent and, in some respects, harder to predict. Risks are no longer neatly separated into market, operational or governance categories. Increasingly, they cut across those boundaries.

This is particularly visible in operational resilience. It is no longer a narrow technical issue. It is a strategic issue for leadership, a supervisory issue for authorities, and, in some scenarios, a systemic issue for markets more broadly.

Operational resilience: a strategic issue for CCP leadership

Operational resilience remains at the top of ESMA's agenda, and I suspect it remains near the top of yours as well.

That is for good reason. CCPs are becoming more digital, more interconnected and more reliant on complex service ecosystems. These developments bring clear benefits, including scalability, efficiency and access to new capabilities. But they also reshape the vulnerability profile of critical infrastructures.

At the same time, cyber threats are evolving in sophistication, speed and potential impact. They are also increasingly linked to the broader geopolitical environment. In other words, cyber resilience is no longer just about protecting systems. It is about preserving trust in market infrastructure under adverse conditions.

Recent discussions around Frontier AI-related developments such as Mythos are a useful reminder of how quickly the technological frontier can move. Whether or not particular scenarios materialise in the near term, the broader lesson is clear: the time available to understand emerging threats and adapt risk controls may be shrinking.

For me, this has three implications.

First, operational resilience must be owned at the top.

This is not a topic that can sit in a technical silo. It requires board attention, senior management accountability and a firm-wide understanding of critical functions and dependencies.

To put it bluntly: if a CEO cannot have a clear conversation about their institution's technological risk profile, critical dependencies or resilience strategy, that would be a concern. Do not worry, there is still no exam at the end of this speech, and this is not a surprise inspection. But the point matters. Operational resilience today is a leadership issue.

Second, third-party risk needs to be treated with much greater realism.

Many CCPs rely on external providers for cloud services, software, connectivity, data and other critical functions. That can bring important benefits. But it can also create dependencies that are difficult to monitor, difficult to substitute and even more difficult to unwind under stress.

This is why third-party risk is moving higher on the supervisory agenda, including under DORA, under EMIR 3 implementation discussions, and at the international level. The key question is not simply whether a function is outsourced. It is whether the CCP understands the criticality of the service, the concentration implications, the legal and operational constraints, the exit options, and the resilience of the provider itself.

Third, resilience must be immediate, but also forward-looking.

In the EU, DORA is now an important anchor for ICT risk management, governance, testing and incident handling. But DORA should not be approached as a compliance exercise. Its real value lies in whether it strengthens decision-making, improves preparedness and sharpens accountability.

At the same time, European work needs to be seen in an international context. Under CPMI-IOSCO, important work is progressing on cyber resilience for FMIs and on FMI dependencies on third-party service providers. This matters because many of the operational risks CCPs face are global in origin, cross-border in transmission, and systemic in effect.

We therefore need consistency not only within Europe, but also in how we think about resilience internationally. A fragmented approach to global operational risk would not be a very resilient outcome.

The practical takeaway is simple. Cloud migration, technology modernisation and digital transformation may improve resilience in some respects. But they also introduce new vulnerabilities. There is no automatic resilience dividend from adopting new technology. The benefits only materialise if governance, controls and recovery capabilities keep pace.

Innovation: strategic opportunities, but also new vulnerabilities

Let me now turn to innovation more broadly. CCPs are operating in a world where AI, cloud, tokenisation, distributed ledger technology and quantum computing are increasingly relevant. Some of these technologies are already being deployed. Others are still emerging. But all of them raise strategic questions for infrastructures that sit at the centre of the financial system.

These technologies may improve efficiency, scalability, collateral mobilisation and analytical capacity. They may support new services and new market structures. But they may also create new forms of operational risk, legal uncertainty, concentration and systemic correlation.

AI

Artificial intelligence may support surveillance, forecasting, optimisation and operational processes. But it also raises questions around transparency, explainability, governance and model risk.

There is also a broader systemic question. If many firms rely on similar models, similar datasets or similar decision frameworks, AI could reinforce common behaviours in stressed conditions. In other words, it may not only improve efficiency; it could also increase correlation. So we should be careful not to assume that more powerful tools automatically mean more resilient outcomes.

Cloud

Cloud can support agility and modernisation. But it can also deepen reliance on a small number of critical providers. That raises questions around concentration, substitutability, contractual leverage, portability and recovery. This is one of the reasons cloud belongs in the operational resilience discussion, not only in the innovation discussion.

Tokenisation

DLT and tokenisation may reshape aspects of collateral management, settlement and post-trade processing. But they do not remove the need for the core functions CCPs provide, including multilateral netting, centralised risk management and the support of financial stability. In that sense, I see these developments as more likely to reshape the way infrastructure service is provided than to replace them.

Still, the legal and operational questions are significant. In relation to tokenised collateral, we need clarity on rights, control, enforceability, segregation, finality and treatment in default. We also need to understand how control works in practice. If effective access depends on keys, governance protocols, interoperability arrangements or external platforms, then those features become relevant for CCP risk management. For a CCP, the question is not whether an

instrument is technologically advanced. The question is whether it remains legally robust, operationally controllable and resilient under stress.

Quantum

Finally, quantum computing is still at an earlier stage, but it already deserves attention. Its potential implications for cryptography and data security mean it should be part of long-term resilience planning. It may not be tomorrow morning's problem, but it is no longer a purely theoretical one either.

What this means for CCPs and for supervisors

What follows from all of this? For CCPs, I think the message is straightforward: innovation should be approached with openness, but also with discipline. The strategic question is not simply how to adopt new technologies, but how to do so without weakening resilience, governance or legal certainty.

For supervisors, the message is equally clear. We need to remain technologically informed, operationally credible and internationally connected. We need to understand where innovation genuinely improves resilience and efficiency, and where it may generate new risks that are insufficiently visible at first sight.

That is also why EMIR 3 matters in this broader context. EMIR 3 is not only about technical amendments. It is part of ensuring that the EU clearing framework remains robust, forward-looking and capable of addressing evolving risks - including in governance, third-party arrangements and margin-related resilience.

Our approach at ESMA remains technology-neutral, but risk-sensitive. We want innovation where it enhances efficiency, resilience and competitiveness. But we also want clarity of responsibility, sound governance and credible controls. Because in the end, technology may change many things, but it does not eliminate accountability.

Conclusion

Let me conclude. The six priority areas in ESMA's CCP heatmap - cyber and operational resilience, market risk, procyclicality, governance and controls, financial innovation, and business risk - together provide a clear picture of the challenges now facing CCPs.

They point to a risk environment that is more complex, more dynamic and more interconnected than before. Or, to put it in simpler terms: I do not think any of us should be overly concerned about a shortage of work in the near future.

In this environment, operational resilience is becoming even more central. And as innovation accelerates, the need for strong governance, clear accountability and realistic risk management only becomes greater.

At ESMA, we remain committed to supporting a framework that is resilient, proportionate and open to innovation. That means effective supervision, strong international cooperation, and a continued effort to keep our own supervisory capabilities aligned with the speed of change.

But this is a shared effort. The resilience of the clearing ecosystem depends not only on rules and oversight, but also on the strategic choices made by CCPs — by your institutions, your boards and your leadership teams. Your engagement, your judgement and your preparedness will therefore remain essential.

Thank you very much.