Elizabeth McCaul: Supervisory expectations on cloud outsourcing

Speech by Ms Elizabeth McCaul, Member of the Supervisory Board of the European Central Bank, at the KPMG Cloud Conference 2024, Frankfurt am Main, 17 October 2024.

* * *

Introduction

It is my great pleasure to speak today at the KPMG Cloud Conference 2024. It is a pity that I cannot be with you in person, but I am sure that you are having a wonderful conference.

There is no doubt that cloud outsourcing offers opportunities to scale operations efficiently, reduce costs and enhance flexibility by leveraging cloud providers' advanced infrastructure and services. Indeed, using the cloud can be a viable strategy for banks to reduce the complexity of their IT operations, which would be a welcome development. But it also introduces new risks and new challenges, including preparing IT systems for use in a cloud environment.

In particular, it presents risks related to IT and data security and vendor lock-in which, if not properly managed, could lead to operational vulnerabilities and business disruptions.

I would like to make three main points in my speech today.

First, cloud outsourcing is rapidly transforming the banking sector, with a significant rise in adoption and expenditure. But it also increases banks' risk exposure, which demands heightened responsibility and robust governance frameworks.

Second, when adopting cloud strategies, banks should retain full accountability for outsourced services, ensuring clear roles, rigorous risk management and appropriate IT security measures.

Third, our supervisory expectations should not be seen as regulatory hurdles, but as strategic enablers to enhance resilience, operational continuity and data protection in banks' cloud strategies.

Relevance of the cloud

Cloud services are transforming the economic landscape and reshaping traditional business models. According to a report by Gartner, worldwide end-user spending on public cloud services is forecast to grow by 20.4% to total USD 675.4 billion in 2024[1], driven largely by sectors like banking. In our own stocktake, we have found that essentially all significant institutions under our supervision use cloud services. Cloud services account for approximately 15% of all outsourcing contracts, with half of these contracts covering the outsourcing of critical or important functions. Moreover, cloud expenses are among the fastest-rising outsourcing costs. But with this growth comes increased responsibility.

Third-party risk management, including cloud outsourcing, is high on the list of the ECB's supervisory priorities for 2024-26 and we expect banks to establish robust outsourcing risk arrangements to proactively tackle any risks that might lead to disruption of critical activities or services.

The ECB's supervisory expectations

We published our draft Guide on cloud outsourcing for public consultation in June this year. The public consultation was open until mid-July and we are now assessing all of the comments.

In total, we received 698 comments from 26 respondents, and there was a strong focus on governance aspects. The main respondents were banking associations, although cloud service providers, individual banks and other industry associations also contributed to the consultation.

Before I tell you more about the comments, let me first explain what the Guide is all about.

The Guide is consistent with existing regulation such as the Digital Operational Resilience Act (DORA) and aims to promote a level playing field for the supervisory treatment of cloud outsourcing by clarifying our supervisory expectations. The Guide draws on risks and best practices observed by Joint Supervisory Teams in the context of ongoing supervision and dedicated on-site inspections.

At the heart of the Guide is the clear expectation for banks to retain full responsibility for their outsourced services. It is not merely a matter of compliance, but accountability. The management body in each institution should ensure that the roles and responsibilities related to cloud outsourcing are clearly defined, well understood and embedded in both internal policies and contractual agreements with cloud service providers (CSPs).

In line with the requirements under DORA, banks should conduct a thorough pre-outsourcing analysis. This involves a detailed risk assessment that considers the complexities of sub-outsourcing chains, data security risks and potential vendor lock-in scenarios. It is important that banks align their cloud strategy with their overall business strategy, ensuring consistency across governance frameworks.

The Capital Requirements Directive states that banks must have contingency and business continuity plans that ensure they are able to continue operating and limit losses in the event of severe disruption to their business. In doing so, banks should adopt a holistic approach to business continuity, particularly for critical functions. Those measures may include multi-region data centres, hybrid cloud architectures, or even multiple CSPs to enhance resilience. This layered approach is crucial in mitigating the risk of service disruption and ensuring that banks can continue to operate smoothly, even in worst-case scenarios such as a failure of the CSP.

We also place significant emphasis on IT security and data confidentiality. This includes implementing stringent data security measures such as encryption and associated cryptographic key management to protect sensitive information. It is vital that these

measures are regularly reviewed and updated in response to evolving threats. Additionally, we consider it good practice for banks to maintain a clear policy on data location, ensuring that data storage and processing comply with both regulatory requirements and the institution's own risk management policies.

Moreover, we advise banks to subject all cloud services to rigorous testing, including disaster recovery plans. In particular, we say that banks should not solely rely on certifications provided by CSPs but also conduct their own independent checks to validate these critical processes. Indeed, I would highlight that the external certifications provided by CSPs may not always be tested as robustly as banks would hope. Banks should be careful not to be too trusting, like the financial sector was before 2008 when it trusted the credit rating agencies. Regular audits and continuous monitoring of CSPs are essential to verify compliance with agreed standards and to promptly identify any emerging risks.

Robust exit strategies are another important element in the area of cloud outsourcing. Comprehensive exit plans ensure seamless transitions and minimise any potential disruptions. These plans should include clear roles and responsibilities, effective data portability solutions and provisions for business continuity. Regular testing of disaster recovery strategies is crucial, ensuring that both the bank and its CSPs are prepared for various scenarios, including abrupt service discontinuation. I encourage all of you to view these guidelines not as mere regulatory hurdles, but as strategic enablers. Robust governance and risk management frameworks are not just about meeting supervisory expectations – they are about safeguarding the integrity of banks and the trust that depositors put in them.

Let me now turn to some of the comments we have received. Many of them concern the legal nature of the Guide and how it relates to existing regulation. Again, let me be very clear here: the Guide does not establish any new regulatory requirements. It simply sets out our supervisory expectations and provides examples of good practices. Some of the other comments relate to more specific issues, such as the need for backups in separate locations, cloud resilience measures and the definition of concentration risks. We very much welcome this detailed feedback and will adjust the Guide as necessary to clarify our expectations. We plan to have the final version ready by the end of the year.

Conclusion

Let me conclude.

Cloud outsourcing can provide significant opportunities for banks but it also increases their risk exposure. This demands robust governance, comprehensive risk assessments and thorough pre-outsourcing analyses. Our supervisory expectations should not be seen as regulatory hurdles in this regard but as strategic enablers to enhance resilience, operational continuity and data protection in banks' cloud strategies.

I wish you a wonderful rest of the conference today.

[1] Gartner (2024), "Gartner Forecasts Worldwide Public Cloud End-User Spending to Surpass $675 Billion in 2024", *press release*, 20 May.