Joachim Wuermeling: Exploring DORA – the Digital Operational Resilience Act and its impact on banks and their supervisors

Speech by Dr Joachim Wuermeling, Member of the Executive Board of the Deutsche Bundesbank, at the European Savings and Retail Banking Group (ESBG), virtual, 23 September 2021.

* * *

1 Introduction

Ladies and gentlemen,

Friends and colleagues,

In 1974, Reinhard Mey, one of Germany's best-known singer-songwriters, released one of his biggest hits, "Über den Wolken", meaning "Above the clouds".

In the song, the protagonist stands on an airfield watching a plane take off. He imagines that the sky beyond the clouds must be where freedom can be found. In the chorus he sings:

"Above the clouds, freedom must be boundless."

Nowadays one could be tempted to change the words of the chorus to: "Inside the cloud, freedom is boundless." Perhaps it is a little too sketchy to draw a parallel between the freedom above the clouds and the opportunities that come with cloud technologies.

But still, let me focus on another parallel between Reinhard Mey's song and cloud computing. For the protagonist in the song, the sky beyond the clouds seems boundless, probably without any rules. But in reality, of course, there are plenty of international rules for the clouds, for air traffic, and air traffic controllers use rules to keep the airspace organised and, above all, safe. Without rules and oversight, air traffic would never be as safe and reliable as it is today, and it wouldn't offer the freedom of travel we normally enjoy (except when a virus comes along, of course …).

Working in the cloud, having all your data available anytime, anyplace, seems boundless and offers many opportunities. But just like in air traffic, cloud providers and online traffic need rules and oversight in order to be stable and beneficial.

The cloud is just one example of the potential, and also of the risks that come with the digitalisation in the financial sector.

This is where DORA comes into play. With DORA – or, to give the act its full name, the Digital Operational Resilience Act –, the EU has begun to forge an oversight framework for banks' Information and Communications Technologies (ICT) risks and for critical ICT third-party service providers. DORA introduces stricter regulation of ICT service providers, including cloud providers. So you could say DORA brings consistent rules and oversight to the seemingly boundless sky beyond the clouds.

My speech on DORA today will focus on three questions:

First: Why DORA? What's our take from a supervisory and financial stability perspective?

Second: DORA, smaller banks and proportionality: What improvements could DORA deliver?

Third: Third-party oversight and banking supervision: are they two sides of the same coin? How should supervisors interact?

2 Why DORA?

Let's kick off with my first question: Why DORA?

First of all, let me take a global perspective: DORA, which forms part of the EU's digital finance package, takes an increasingly important area of digital finance regulation to the next level. This will open up opportunities for the EU to take a leading role in the field of digital financial services. We could even enhance our digital and financial sovereignty in the EU. By advancing regulation in this field, we have the opportunity to set global standards and remain competitive – while mitigating the risks arising from digital finance.

Second, from my perspective as a banking supervisor at the Bundesbank: DORA addresses today's most important challenges for managing ICT risks at financial institutions and critical ICT third-party service providers. Only if these risks are properly managed can digitalisation truly deliver on the many opportunities it offers for the banking and financial industry: Better analysis and better data management can make banks more resilient. For instance, early warning systems for loan defaults based on automatically evaluated economic news could improve risk management.

I therefore see the role of supervision as a "supporter" of digitalisation in the banking sector. Legislation should not raise the bar for digital innovation, nor should it overburden the financial sector; instead, it should name risks and help institutions manage these risks adequately. This is, of course, within the framework of our supervisory mandate, which provides for technology and market neutrality.

And third, let me put myself in a central banker's shoes: I believe digitalisation can make the financial system as a whole more resilient – provided risks are kept suitably in check. ICT risks continue to pose a challenge to the operational resilience, performance and stability of the EU financial system. This was insistently underlined in a paper published by the Basel Committee on Banking Supervision (BCBS) this Monday.[1]

Only if financial institutions take an independent, sovereign and balanced approach to the opportunities and risks presented by digitalisation can the functioning of the financial system be safeguarded in the long term. If we succeed in mitigating these risks, we even have a chance of making not only individual institutions, but the financial system as a whole more stable with the help of digital tools.

So from all three perspectives – from the global perspective, seeing the EU as a standard setter; from a supervisor's perspective, looking at the stability of individual institutions; and from a central banker's view, looking at the stability of the entire financial system – digitalisation opens up enormous potential for efficient and stable financial markets if risks are properly managed. That's why I strongly support DORA.

3 DORA, smaller banks and proportionality

But of course, since I am speaking to the European Savings and Retail Banking Group today, whose members tend to be somewhat smaller institutions, there is another question that comes up: How can the many small banks we have in Europe leverage the opportunities of digital finance, and how does DORA affect smaller banks?

Let me start off by making a general point: small and medium-sized banks in particular can benefit a great deal from digitalisation if the risks are properly managed. Cloud services enable banks to tap into huge computing capacities and state-of-the-art software capabilities without an expensive IT infrastructure which would exceed their resources. Cloud services can boost big data analytics and artificial intelligence, even more so among small and medium-sized banks. Moreover, cloud service providers can better equip banks to fend off certain types of cybercrime.

Using the cloud can therefore improve smaller banks' access to new technologies.

But nevertheless, there is a clear rule in banking supervision: you can't outsource responsibility. Every bank has a duty to monitor and control the risks arising from an outsourcing relationship. That rule also holds true for smaller banks using the services of cloud service providers.

Many cloud service providers operate internationally, have millions of customers and an enormous amount of data and money. Compared to them, smaller European banks are just too small to be able to really audit the cloud service providers. One current possibility for smaller banks is to work together when auditing cloud providers, in what are known as pooled audits. Banks can and should make even greater use of this cooperative approach.

This is the first efficiency gain that DORA can deliver for smaller banks: systemically important third-party service providers will be audited by public authorities.

This does not mean that the individual bank is off the hook, but central oversight of this kind is certainly a benefit for smaller banks. It could produce synergy effects. The resilience of providers would presumably increase. Institutions would enjoy greater certainty surrounding compliance with regulatory requirements. Maybe, in the end, banks could also base their own supervision on supervisors' inspection and oversight findings and have greater legal certainty when outsourcing operations to the cloud.

But central oversight of cloud service providers is not the only improvement DORA can bring for smaller banks.

My second argument for DORA and smaller banks: lowering the cost of incidents and reducing the administrative burden in incident reporting.

Although it is difficult to estimate the cost of operational incidents in the financial sector, industry research points to a figure of between 2 and 27 billion euro per year for the EU financial sector. DORA could help to lower these numbers and mitigate wider impacts of serious cyber incidents.

With more consistent and standardised incident reporting procedures, DORA could also reduce the administrative burden on financial institutions and increase the efficiency of supervision.

However, standardisation also narrows the scope for implementing rules in a proportionate manner.

This brings me to my third argument: looking especially at smaller banks, proportionality is a key topic in the ongoing negotiations on DORA among EU Member States.

In fact, DORA – being level 1 legislation – should be as principles-based and technology-neutral as possible to allow a quick adaption to new technological developments. Bearing this in mind, proportionality will be an important aim when developing the regulatory standards for implementing the DORA rules. For DORA, then, the objective is to strike the right balance between providing principles and allowing for sufficient and proportionate flexibility.

4 Third-party oversight and banking supervision: two sides of the same coin?

My first point was: Why DORA? My second was: How does DORA work for smaller banks? Le me now turn to my third question: How can third-party oversight and banking supervision cooperate – are they two sides of the same coin?

Let me start with an example of two frameworks that don't yet complement each other well. As banking supervisors, we are particularly interested in processes and applications that have a bearing on risk management, such as artificial intelligence in credit assessments, liquidity planning, or portfolio management. The use of artificial intelligence is supervised under the

existing banking regulation. I am therefore rather critical about introducing special authorisation requirements, such as those proposed by the European Commission for creditworthiness checks. Banks should continue to be supervised in a technology-neutral manner – without duplicating any regulation, and without duplicating supervisory processes.

But let me circle back to the current DORA proposal: the oversight framework for critical ICT third-party service providers does indeed complement the supervisory approaches taken within the Single Supervisory Mechanism (SSM) and at the national level.

While the SSM focuses on the risks that financial institutions take when they outsource activities to ICT third-party providers, DORA enables the European Supervisory Authorities (ESAs) to access critical ICT third-party service providers directly and sanction them if necessary.

For this task-sharing arrangement to work, there are three key requirements for DORA I would like to emphasise from my point as a supervisor:

1. A well designed approach ensuring supervisory efficiency;
2. closer cooperation among authorities and
3. and clear consistency of rules.

First, it is key that we always bear in mind the objective of supervisory efficiency when designing DORA.

The DORA proposal raises some crucial points regarding the interplay between (traditional) banking supervision and the new European oversight framework.

We welcome the aim to streamline and harmonise any overlapping regulatory requirements or supervisory expectations.

If the ESAs increasingly engage in supervising cloud providers, they must ensure that they do so in an efficient manner and without duplicating any work. One issue should be examined only once and by just one authority.

This is important for us as supervisors, as we have a duty to deploy our staff and resources efficiently. And of course, this is important for you, the banks, as well: you don't want to be supervised twice for the same issue. I am sure this is also true for cloud service providers.

This implies that we must clearly define the responsibilities of both banking supervisors and the ESAs in order to avoid a clash of competencies.

Under the proposed regulation, the ESAs will perform operational oversight functions for critical ICT third-party service providers, with the EBA designated as the lead overseer and in close cooperation with EIOPA and ESMA. This includes on-site inspections, ongoing oversight and recommendations for action.

By contrast, banking supervisors are to stick to their mandate of supervising financial institutions. Supervision of critical ICT third-party service providers therefore falls only indirectly, if that, within the scope of banking supervisors.

Second, closer cooperation among authorities is needed.

If the ESAs directly supervise critical ICT third-party service providers, this will make the supervisory landscape more complex and increase the need for cooperation with supervisors.

It is all about striking a balance between (national) supervision and the new European oversight framework after all.

One example of this is the joint examination teams that the ESAs will set up to conduct on-site inspections on the premises of critical ICT third-party service providers: these teams will comprise staff from both the ESAs and the relevant competent authorities.

Moreover, authorities could also cooperate closely when identifying critical ICT third-party service providers and evaluating concentration risk – this is an area where supervisors could contribute valuable information.

Against this backdrop, I strongly support what is proposed under DORA: to prevent future cyber-attacks and reduce ICT threats to the financial system as a whole, we need to strengthen information sharing, and we need to boost cooperation between the ESAs, supervisors and other relevant stakeholders such as the European Union Agency for Cybersecurity.

My third point: the need for consistent rules.

It is important that the rules envisaged by DORA are consistent with the existing rules in banking regulation. Otherwise, this would fragment regulatory standards even further and overburden banks that engage in outsourcing arrangements.

In my view, we need a sound supervisory architecture balancing third-party oversight and banking supervision. Then, these two aspects can become two sides of the same coin: the coin that offers digital opportunities for the financial sector.

5 Closing remarks

Ladies and gentlemen,

to sum up:

First: digitalisation brings opportunities and risks. To help the financial sector seize the opportunities, it is helpful to manage the risks with DORA – from the global view, in terms of setting standards; from the supervisor's view of individual banks; and from the central banker's view in terms of financial stability.

Second: DORA comes with several improvements for smaller banks, but proportionality should be discussed further in the ongoing negotiations.

Third, banking supervision and third-party oversight should be two sides of the same coin, with an efficient institutional set-up, close cooperation among authorities, and consistent rules. We at the Bundesbank will do our part to make this work.

Returning to Reinhard Mey's line that "Above the clouds, freedom must be boundless":

We all want to tap into the digital freedom that lies "beyond the clouds", into using digital technologies with the fewest constraints possible. In this spirit, let us all work together and help DORA set the standards for rules and oversight to make digital freedom and digital resilience possible.

Thank you for your attention.

---

1 See Newsletter on cyber security from BIS: www.bis.org/publ/bcbs_nl25.htm