waterstechnology

By
Emma Hilary Gould
11 Jun 2024

Financial institutions across Europe are determining which third-party vendors underpin their most critical operations as a part of the EU's milestone Digital Operational Resilience Act, which takes effect next January. The second batch of the Dora regulatory technical standards (RTS) is due to be released on July 17, and industry participants are hoping it sheds more light on which third-party vendors will be designated as critical, both at the individual bank level, and at the industry level.

The first batch of technical standards was finalized this past January as part of Dora's mandate that the European Supervisory Authorities jointly develop 13 policy instruments to clarify how the bill will be enforced. It included technical standards on information and communication technology risk management frameworks, criteria for classifying ICT-related incidents, and establishing templates for information registers, which financial institutions will use to track their use of ICT third-party providers.

The designations have important implications for how the act will be carried out, from protocols around resilience testing within a bank to specifications for EU authorities to oversee vendors deemed systemically critical to the finance industry, such as cloud providers like Microsoft Azure, Amazon Web Services, and Google Cloud. Some say the current vagueness in Dora's definition of "critical" has made negotiations difficult between third parties and the financial institutions that use them.

Beate Zwijnenberg, global chief information security officer at ING, says many want EU regulators to release more information on the third parties expected to be in Dora's scope. Without this, she notes many vendors are avoiding compliance with Dora, citing Article 31, which restricts the act's application to ICT providers, defined broadly in the bill as vendors regularly offering digital and data services, a definition that some industry groups have also criticized as being too vague. "[They say:] 'In our opinion, we're not delivering ICT services according to the Article 31 in Dora.' And I said, 'In my opinion, you are,'" Zwijnenberg says.

As noted before, a vendor's criticality will be evaluated on two levels—its function within individual institutions and at an industry level. The industry-level criticality depends on the number of financial institutions using a given third party. If many financial entities use a given third party—as is the case for the trio of major cloud providers—those third parties will come under direct regulatory oversight, although it is unclear which body, or bodies will serve as the regulatory authority. This list of industry-critical vendors has yet to be released, and with no publicly known due date, there is uncertainty over whether some widely used providers will also be deemed critical.

The second level of criticality will be determined by individual financial entities. Each institution must declare which vendors underpin their critical business functions, defined broadly as those functions that could jeopardize the operations of the entire institution if were they to fail. A designation at the institutional level would see certain vendors come under stricter contract clauses under Dora's Article 30, says John Salmon, a partner at law firm Hogan Lovells. "What it will mean is—and we find this already all the time with [European Banking Authority]—is that where you're dealing particularly with vendors outside Europe, they're going to ask whether they must comply," he says. "It can be quite time-consuming and expensive to then negotiate a contract where they're saying, 'I don't know about this; why do I have to do this?'" As part of the regulation, financial institutions will send regular reports on their usage of critical third parties to the supervisory authorities. These information registers will inform which industry-critical providers will be subject to direct regulatory oversight under a yet-to-be-created body.

In a statement released on May 22, the Association for Financial Markets in Europe (Afme) said the incoming registers introduce new manual tasks for financial institutions and may be difficult to accurately complete if third parties do not want to comply. Designations at the bank level can also vary depending on an institution's interpretation of criticality. One bank could list 10 critical functions, while another bank may list 60. Peter Hainz, global head of cloud and security strategies at reconciliations provider SmartStream, notes that one bank might view the vendor's back-office services as critical while another bank may not. Zwijnenberg says that for a bank that has outlined more critical functions than a peer, the cost and time required for carrying out certain provisions of Dora could increase. For example, Dora requires that a bank complete threat-led penetration testing, a type of cyber testing that simulates current hacking techniques in a live environment, across its critical functions. More critical functions would expand these testing obligations.

In an open letter, the European Cloud User Coalition noted that certain Dora criteria around the criticality of vendors could be improved by basing the systemic impact of a third party on the size of the entities using it, rather than the number of them using it. Further, the letter noted that the register of information has yet to be finalized, and that the information

requested in the registers is too detailed. While questions remain over the role of financial entities and their third parties under Dora, Zwijnenberg and Salmon say the act is going in the right direction, so long as regulators listen to market participants and provide more detail. “The whole idea behind this legislation is to give the financial entities more comfort that they’ve got a rigorous contract or, where there’s a critical ICT service provider, that they are directly regulated,” Salmon says.