Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How Regulation Of Tech Providers Is Breaking New Ground

By **David Berman and Emily Lemaire** (July 19, 2024, 4:16 PM BST)


David Berman


Emily Lemaire

With the incoming regimes of the European Union regulation on digital operational resilience for the financial sector, or DORA, effective January 2025, and the U.K. regime for critical third parties expected to apply from early to mid-2025, EU and U.K. financial services regulators are breaking new ground by expanding the application of financial services regulation to select technology providers.

As the landscape in which financial institutions operate evolves, e.g., through the rapid development of technologies such as generative artificial intelligence, the growing sophistication of cybercrime and significantly increased reliance on third-party information and communication technology service providers, financial institutions and the financial system more broadly face a heightened risk environment.

It is in this environment that the U.K. and EU financial services regulators have each identified an important gap in their regulatory frameworks.

The existing operational resilience obligations in place in the U.K. and EU allow for the supervision of financial institutions and their arrangements with third-party providers and provide for associated enforcement sanctions on such financial institutions.

In other words, current regulatory outsourcing requirements apply directly to the financial institutions, but not to the third-party providers. However, given the ever-increasing dependency of financial institution on certain third parties, this is no longer deemed to afford a sufficient degree of protection to the stability of the financial system.

The EU DORA and U.K. critical third-party regimes will see certain information and communication technology service providers designated as critical to the sustained delivery of financial services across the region — and thus subjected to the direct oversight and enforcement jurisdiction of the financial services regulators.

In this article, we provide an overview of the criteria and expected timing for designation under each regime, a comparative overview of the requirements that will apply to designated third parties operating in the U.K. or EU, and guiding questions that prospective designated technology providers can consider ahead of increased engagement with financial services regulators.

Designation Under Each Regime

At this stage, certain providers that service multiple financial institutions will effectively know whether they will be designated under the U.K. critical third-party regime or EU DORA, e.g., by virtue of early regulatory engagement.

U.K. Critical Third-Party Regime

HM Treasury may designate a third-party provider as critical by applying the following two broad criteria:

- Materiality: How important are the services to delivery of financial services that are essential to the U.K. economy or to the stability of, or confidence in, the U.K. financial system?

- Concentration risk: How many and what type of financial institutions, and financial market infrastructure, are provided the relevant services by the third party?

In contrast with EU DORA, there is limited guidance on how the designation criteria will be applied in practice, with no set thresholds in place. Rather, the decision to designate a provider as critical is at HM Treasury's sole discretion, such that HM Treasury may choose to designate a third party without receiving a recommendation to do so from a U.K. financial regulator, although in practice we do not expect this to happen often — if ever.

There is an approximate six-month process for a third party to be designated as critical. As the rules around designation are now in force, this process could technically begin at any point. However, the regulatory rules with which designated firms will need to comply are not yet finalized and specific timings for enforcement of these obligations are still unclear.

EU DORA

The EU DORA designation process is more prescriptive. While the European supervisory authorities must designate a firm as critical in accordance with a set of criteria that revolve around the same overarching concepts as the U.K. critical third-party regime. i.e., materiality and concentration risk, these criteria must be applied in accordance with Commission Delegated Regulation (EU) 2024/1502.

This regulation is secondary legislation that came into force on June 19, supplementing the designation criteria with technical qualitative and quantitative subcriteria.

Now that this secondary legislation has come into force, the designation process may begin at any point, although direct obligations, including the regulators' supervisory powers, will not apply until Jan. 17, 2025.

Requirements for Management of Operational Risk

U.K. Critical Third-Party Regime

The regulators have proposed the application of a two-tier approach to critical third parties:

- Six high-level fundamental rules, applicable to all services provided to financial institutions by a designated third-party; and

- Eight detailed operational risk and resilience requirements, applicable only to the material services that resulted in the third party's designation.

In addition, the regulators propose testing requirements on the designated third party, including in relation to specific scenarios and the third party's financial sector incident management playbook, a document setting out how the business would communicate with and support the regulators and customers during an incident affecting its services.[1]

EU DORA

While the requirements for the management of operational risk under Articles 28-30 of EU DORA apply only to financial institutions, the lead overseer of a designated third party will annually assess that the business has in place comprehensive, sound and effective rules, procedures, mechanisms and arrangements to manage information and communication technology risk.

Based on its assessment, the lead overseer may issue recommendations to the designated third party. In practice, these recommendations will effectively be mandatory.

Partial or full noncompliance by the designated third party could lead to monetary penalties, which may be publicized by the lead overseer. Ultimately, the temporary or permanent prohibition of financial institutions from using the designated third party's services may be imposed in part or completely by national authorities.

Additionally, both designated and undesignated third-party providers will indirectly be affected by the obligations applicable to financial institutions, as financial institutions' commercial expectations for third parties will shift to comply with the heightened oversight obligations under the DORA.

Therefore, third-party providers should expect requests to renegotiate contractual arrangements, increased auditing and interrogation of their risk management frameworks, including their general approach to risk, from financial institution customers.

The European Central Bank recently published a draft version of its "Guide on outsourcing cloud services to cloud service providers."[2] This is addressed to ECB-regulated banks, but should be carefully considered by cloud service providers, as it details onerous indirect expectations of such providers.

As an example, the ECB has asserted that banks should ensure that cloud service providers establish equivalent risk management practices, processes and controls as would otherwise be adopted by banks.

The significance of this statement is not to be underestimated, as many cloud service providers are unlikely to have the governance and internal control frameworks that are equivalent to those operated internally by a bank. The ECB accepted comments on its draft guide until July 15, and we expect significant representation from relevant stakeholders, including both banks and cloud service providers.

Local Establishment Requirements

U.K. Critical Third-Party Regime

There is no requirement for a designated third party to set up an establishment in the U.K. However, the regulators have suggested that non-U.K. parts of the business that offer relevant services will likely be

subject to the regulators' supervisory remit.[3]

EU DORA

A designated third party must establish an EU subsidiary within 12 months of designation.[4] However, as has been suggested under the U.K. critical third-party regime, non-EU parts of the business that offer relevant services will be subject to the lead overseer's supervisory remit.[5]

Provision of Information Requirements

U.K. Critical Third-Party Regime

The regulators will have wide information-gathering rights over the designated third party, including the ability to conduct investigations and inspections, or to commission a skilled person to assess the business' compliance with the U.K. critical third-party regime requirements.[6]

EU DORA

The lead overseer will have wide information-gathering rights over the designated third party, including the ability to conduct investigations and inspections over the designated third party.[7]

Reporting Requirements

U.K. Critical Third-Party Regime

The designated third party will be required to submit a self-assessment to the regulator within three months of designation, and annually thereafter.

EU DORA

An assessment of the third party will be performed by the lead overseer, as referenced.

Notification Requirements

U.K. Critical Third-Party Regime

Designated third parties will be required to notify the regulators and financial institution customers of relevant incidents that affect their services. This will involve a phased incident notification process.

EU DORA

Designated third parties will be contractually required to notify financial institutions of such incidents, and the financial institutions in turn will need to follow a phased incident notification process to alert the regulators and their customers.[8]

Fees

U.K. Critical Third-Party Regime

No fees have been suggested, thus far.

EU DORA

The lead overseer may charge the designated third party a fee for its oversight activities, calculated in accordance with secondary legislation that came into force on June 19.[9]

Preparing for Increased Contact

Designated technology providers are entering a brave new world of direct scrutiny by financial services regulators.

Given the importance with which the regimes are being treated within the EU, as well as the U.K. regulators' supervisory priorities, plus the potential harm that regulators perceive technology providers pose to the stability of the financial system, we envisage the depth and sophistication of such scrutiny to be greater to that experienced by information and communication technology providers during customer audits.

Firms should consider the following initial guiding questions prior to any regulatory engagement under either regime: Has the firm embedded operational risk management at each stage of the product or service life cycle? Is this formally documented and overseen?

In practice, the U.K. critical third-party regime and EU DORA will likely require information and communication technology providers, over time, to adapt, refine or better document their overall approaches to risk, governance and accountability.

For instance, information and communication technology providers will not typically operate a so-called three-lines-of-defense risk management model, as financial regulators would ordinarily expect from financial institutions. It will therefore be important for financial institutions to be able to articulate and demonstrate to financial regulators that their existing risk-management approaches nevertheless operate effectively.

Information and communication technology providers will likely experience a particular focus by financial regulators on process, documentation, governance and accountability.

Can the firm comprehensively explain and evidence the risk management model that is operated in relation to the relevant services, and link the governance and oversight arrangements in relation to this model? Technology providers must be prepared to work with regulators to help them understand how their business model, the risk management framework and oversight thereof, function.

It would be helpful for technology firms to be preparing comprehensive documents setting out their risk management framework and governance arrangements ahead of regulatory engagement.

Does the firm have the correct strategic approach to engaging with financial services regulators? It is important, from an early stage, to build good rapport with regulators — to show that the firm is willing to be transparent and collaborative, to the extent required under the regimes.

Where a firm is subject to a regulatory examination or investigation — this should not be treated as a routine client audit — not least because of the potential direct regulatory penalties, indirect financial

institution customer fallout, or reputational damage.

Who can the firm designate as the point person for dealings with the regulator? This is an important role and should, ideally, be a senior person supported by relevant senior-level business stakeholders.

How will the oversight of dealings with the regulator work? Firms should ensure sufficient management oversight of any dealings with the regulator. This requires regular reporting to and challenge from senior management during the course of any regulatory dealings — not simply at the start and end. For instance, a centralized regulatory affairs office is one model that several information and communication technology providers are actively considering.

Conclusion

The impending direct application of financial services regulation and supervision to designated technology providers of services to financial institutions represent a significant development that is not to be underestimated by technology firms or, indeed, financial institutions themselves.

This article offers some practical guidance for those firms about to enter this brave new world of financial services regulation and oversight. The clock to commencement is ticking fast and preparations should commence in earnest.

David Berman is a partner and Emily Lemaire is an associate at Covington & Burling LLP

[1] Joint consultation paper (CP26/23).

[2] https://www.bankingsupervision.europa.eu/legalframework/publiccons/pdf/ssm.pubcon240603_draftguide.en.pdf.

[3] Joint PRA and FCA discussion (https://www.bankofengland.co.uk/prudential-regulation/publication/2022/july/operational-resilience-critical-third-parties-uk-financial-sector) and consultation (https://www.bankofengland.co.uk/prudential-regulation/publication/2023/december/operational-resilience-critical-third-parties-to-the-uk-financial-sector) papers.

[4] Article 31 of EU DORA.

[5] Article 36 of EU DORA.

[6] Section 312P of FSMA 2000, as amended by FSMA 2023.

[7] Articles 35, 37 to 39.

[8] Articles 17 to 23 of EU DORA.

[9] Commission Delegated Regulation (EU) 2024/1505.