EU RegCORE Client Alert

Financial Services

August 2026

From outsourcing to infrastructure: Comparing DORA to the UK's Critical Third Party Regime

QuickTake

As financial institutions continue to operationalise the EU's Digital Operational Resilience Act (**DORA**),[1] attention is increasingly turning to the United Kingdom's Critical Third Party (**CTP**) regime, with new CTP designations published 13 July 2026.[2] Although both frameworks seek to strengthen operational resilience by introducing direct oversight of systemically important technology providers, they differ in their legal architecture, supervisory philosophy and implementation.

Those differences matter for firms operating across both jurisdictions. Yet they also reveal something more fundamental. Both regimes reflect a broader shift in financial regulation: the expansion of the regulatory perimeter beyond regulated financial institutions to encompass the digital infrastructure upon which modern finance depends.

Dr. Michael Huertas
Tel: +49 160 97375760
michael.huertas@pwc.com

Fabian Joshua Schmidt
Tel: +49 1514 1490437
fabian.joshua.schmidt
@pwc.com

EU RegCORE Team
de_regcore@pwc.com

[1] For a detailed overview of DORA please see our dedicated series on our EU RegCORE.
[2] Details available here.

For internationally active firms and critical technology providers alike, understanding where the regimes converge - and where they diverge - will become increasingly important.

Same Objective, Different Regulatory Philosophies

At their core, both regimes recognise that certain information and communication technology (**ICT**) providers have become so deeply embedded within the financial sector that resilience can no longer be managed solely through outsourcing requirements imposed on regulated firms.

Historically, responsibility rested entirely with the financial institution. Today, regulators increasingly seek direct engagement with the providers themselves. The policy destination is therefore broadly aligned. The regulatory journey is not.

DORA: Operational Resilience as Prudential Supervision

The EU's approach is comprehensive. DORA integrates oversight of Critical ICT Third-Party Providers (**CTPPs**) into a broader operational resilience framework that includes governance, ICT risk management, incident reporting, testing, concentration risk management and supervisory cooperation. Oversight is led by the European Supervisory Authorities (**ESA**s) through a Lead Overseer model supported by Joint Oversight Forums. Technology resilience becomes part of prudential supervision itself. On 18 November 2025, the ESAs designated 19 CTPPs.[3]

The UK: Systemic Risk Through a Financial Stability Lens

The UK's CTP regime adopts a narrower and more principles-based approach. Rather than replicating DORA, the regime supplements the existing operational resilience framework administered by the Financial Conduct Authority (**FCA**), the Prudential Regulation Authority (**PRA**) and the Bank of England (**BoE**) by allowing direct oversight of designated technology providers whose disruption could threaten UK financial stability.

Why critical third parties matter

CTPs are third party providers whose service disruption or failure could threaten the stability of, or confidence in, the UK financial system. They may include technology, data and operational service providers of critical services to regulated firms and financial market infrastructures (**FMIs**). Financial services firms include all firms authorised by the PRA and/or the FCA and UK authorised branches of third-country firms. FMIs include central securities depositories (**CSDs**), central counterparties (**CCPs**), UK recognised investment exchanges (**RIEs**), recognised payment systems operators (**RPSOs**) and specified service providers (**SSPs**) to RPSOs.

Firms and FMIs have become increasingly reliant on third-party service providers (such as cloud-based service providers, including Amazon, Microsoft and Google) through their outsourcing and other contractual arrangements. If a provider that supports a significant part of the financial sector experiences serious disruption to its services, it could affect many firms, consumers and markets. The CTP regime helps regulators address these risks that could impact the wider financial system.

Well-managed outsourcing and other arrangements can bring many benefits to firms, including efficiency gains, reduced costs, scalability, faster innovation, better customer outcomes and improved operational resilience. However, they can also pose risks to individual firms, the regulators' objectives and the wider financial system. These risks stem from a combination of firms' growing dependency on third parties for

[3] See our Client Alert available here.

services whose failure or disruption could have a systemic impact, concentration in the provision of these services (as of 2020, over 65% of UK firms used the same four cloud service providers (**CSPs**) for cloud infrastructure services), and the potential impact of service failure on market integrity and financial stability.

Disruption to any systemic services that certain third parties provide to firms could therefore lead to a single-point-of-failure that may simultaneously impact multiple firms, their counterparties, customers and direct participants (even if they do not directly rely on the relevant third parties' services) and, in extreme cases, the financial stability of the UK.

A new oversight regime

The regime has been established by way of the Financial Services and Markets Act 2023 (FSMA 2023). Section 18 of FSMA 2023 amended Part 18 of the Financial Services and Markets Act 2000 (FSMA), including by inserting a new chapter 3C (Critical Third Parties) into FSMA. Under the new oversight regime, HM Treasury is empowered to designate certain third-party service providers as "critical", while the financial regulators are empowered to make rules, gather information and take enforcement action against CTPs.

In November 2024, the FCA, Bank of England, and PRA (the **UK regulators**) published their joint policy statement (PRA PS16/24 / FCA PS24/16), confirming their final policy regarding oversight of CTPs' operational resilience. The regulatory rules took effect from 1 January 2025. The rules apply to a CTP from the date the relevant Treasury designation regulation comes into force.

The UK regulators' final rules for CTPs are contained in: a new Critical Third Parties sourcebook (**CTPS**) in the FCA Handbook; a new Critical Third Parties Part of the PRA Rulebook; and a new Critical Third Parties Part of the BoE FMI Rulebook. A joint BoE/PRA/FCA supervisory statement (SS6/24) is the key source of guidance for CTPs on how to approach, comply with, and interpret the regulators' requirements.

In addition to the core rules and guidance, HM Treasury has published the regulators' memorandum of understanding (**MoU**), which sets out how they intend to co-ordinate the exercise of their respective functions under the CTP oversight regime. The regulators have also issued a CTP approach document that sets out how they intend to use their oversight powers for CTPs and have established a joint CTP Consultation and Coordination Forum (**CCF**).

Through proportionate, targeted, and coordinated oversight of systemic services provided to firms by CTPs, the UK's CTP regime aims to:

- Reduce systemic risk by ensuring CTPs meet robust operational resilience standards.
- Enable regulators to intervene and raise the resilience of services provided by CTPs.
- Complement, not replace, firms' own responsibilities for managing third-party risks.
- Encourage timely information sharing between CTPs and firms, to ensure that firms have the appropriate knowledge to adequately manage risks related to their use of CTP services.
- Oversight may include regulatory engagement, information gathering and resilience assessments focused on the systemic services CTPs offer to the UK financial sector.

What the regime means for designated CTPs

Joint oversight of CTP services begins when the Treasury's designation regulations come into effect, meaning the regulators' rules apply to CTPs from then. The regulators' targeted oversight prioritises the systemically important third-party services, not the entirety of CTPs' businesses, ensuring a proportionate approach to managing systemic risks. CTPs must submit an interim self-assessment to the regulators within three months of designation and an annual self-assessment every year thereafter.

The UK regulators have introduced a set of six CTP Fundamental Rules that provide a general statement of a CTP's fundamental obligations under the oversight regime. These require CTPs to: (a) conduct business with integrity; (b) act with due skill, care and diligence; (c) act in a prudent manner; (d) have effective

risk strategies and risk management systems; (e) organise and control affairs responsibly and effectively; and (f) deal with regulators in an open and co-operative way.

The regulators have also introduced eight Operational Risk and Resilience Requirements that articulate the standards of resilience CTPs must maintain. These cover: (1) Governance; (2) Risk management; (3) Dependency and supply chain risk management; (4) Technology and cyber resilience; (5) Change management; (6) Mapping; (7) Incident management; and (8) Termination of services. While more granular than the Fundamental Rules, these Requirements are outcomes-focused, specifying objectives CTPs must achieve without prescribing how they should be met.

CTPs are required to carry out regular scenario testing of their ability to continue providing each systemic third party service within their appropriate maximum tolerable level of disruption in the event of a severe but plausible disruption. They must also maintain and operate an incident management playbook (within 12 months of designation) and undertake incident management playbook exercises with a representative sample of firms at least biennially.

What the regime means for firms

Firms remain responsible for managing their own third-party risks in line with existing operational resilience and outsourcing requirements. The CTP regime complements but does not replace firms' existing obligations. Firms may, however, obtain benefits from the establishment of the CTP regime. Requiring CTPs to ensure that any systemic third party services they provide meet minimum resilience standards, and testing the resilience of these services, could strengthen firms' ability (both individually and collectively) to oversee and obtain assurance from the CTPs they rely on.

How CTPs are designated

The Treasury decides whether to designate a third party as a CTP, based generally on recommendations from the regulators. The Treasury may also make designations without any regulator recommendations. The Treasury can de-designate CTPs or designate new CTPs as markets evolve. Under FSMA, HM Treasury may only designate a third party if, in its opinion, a failure in, or disruption to, the provision of those services could threaten the stability of, or confidence in, the UK financial system.

FSMA provides that HM Treasury must take into account two high-level criteria when forming its opinion: **materiality** (the materiality of the services provided by the third party to firms' delivery of activities, services or operations that are essential to the UK's economy or financial stability) and **concentration** (the number and type of firms to which the third party provides services). HM Treasury expects to take around six months to process recommendations for designations received from the regulators.

Once designated by the Treasury, CTPs' systemic services are jointly overseen by the regulators. A "systemic third party service" is defined as a service (wherever carried out) provided by a CTP to one or more firms, a failure in or disruption to which could threaten the stability of, or confidence in, the UK financial system. Before making any designation regulations, HM Treasury must consult each of the relevant financial regulators and notify the person to be designated in writing, specifying a reasonable period within which that person may make written representations.

Designated Critical Third Parties

On 13 July 2026, HM Treasury designated the following entities as CTPs:

1. Amazon Web Services EMEA SARL[4] - also designated as an EU CTPP;
2. Google Cloud EMEA Limited[5] - also designated as an EU CTPP;

[4] Designation details available here.
[5] Designation details available here.

3. Microsoft Ireland Operations Limited[6] - also designated as an EU CTPP; and
4. Oracle Corporation UK Limited[7] - not designated as an EU CTPP but its affiliate Oracle Nederland B.V. is designated as an EU CTPP.

From their designation date, these CTPs are subject to oversight by the BoE, the PRA and the FCA to ensure they have robust arrangements in place to identify, manage and recover from operational disruptions affecting critical services used across the financial services sector. Compliance with certain requirements in the regulators' rules will be subject to a transitional period that will start from the date HM Treasury specifies in a designation order.

Enforcement powers

FSMA gives the financial regulators a range of enforcement powers in relation to CTPs. If a financial regulator considers that a CTP has breached a relevant requirement, it may: publish a statement (censure) to that effect; prohibit the CTP from entering into arrangements, or continuing, to provide services to firms; prohibit firms who receive services from the CTP from continuing to receive those services; prohibit firms from entering into arrangements to receive services from the CTP; impose conditions or limitations on the CTP's provision of any services to firms; and impose conditions or limitations on the services firms receive from the CTP. FSMA does not, however, provide the regulators with a power to impose a penalty or fine on CTPs.

Incident reporting

The UK regulators have introduced a phased approach to incident reporting. A "CTP operational incident" is defined as either a single event or a series of linked events that causes serious disruption to the delivery of a systemic third party service, or impacts the CTP's operations such that the availability, authenticity, integrity or confidentiality of assets belonging to firms is or may be seriously and adversely impacted. CTPs must submit: an initial incident report (as soon as practicable after occurrence); intermediate incident reports (as needed following significant changes); and a final incident report (within a reasonable time, normally 30 working days, of resolution). By contrast, DORA prescribes specific timeframes: financial entities must submit an initial notification within 4 hours of classifying a major ICT-related incident, an intermediate report within 72 hours, and a final report within one month of resolution.

Comparing the frameworks

The most significant divergence between the EU's DORA regime for CTPPs and the UK's CTP regime under the Financial Services and Markets Act 2023 lies in where the compliance burden sits: DORA imposes a detailed, prescriptive contractual code that financial entities must build into their agreements, whereas the UK regime places resilience obligations directly on the designated CTP through regulatory rules, leaving firms' contractual relationships governed largely by pre-existing outsourcing and operational resilience requirements (SYSC 8 and the Operational Resilience Policy Statement/SS2/21).

Topic	EU DORA (CTPP)	UK CTP Regime	Key considerations
Primary objective	Digital operational resilience across the EU financial sector	Protection of UK financial stability	**Firms:** Align resilience frameworks to primary regulatory objective.

[6] Designation details available here.
[7] Designation details available here.

Topic	EU DORA (CTPP)	UK CTP Regime	Key considerations
			Providers: Understand whether oversight focuses on your resilience (UK) or broader digital resilience ecosystem (EU).
Legal basis	Directly applicable EU Regulation	FSMA 2023 and secondary legislation	**Firms:** DORA is directly applicable; UK regime requires monitoring of secondary legislation. **Providers:** EU establishment may be required under DORA; UK regime is location-agnostic.
Who designates providers?	ESAs (EBA, ESMA, EIOPA) designate CTPPs based on systemic criteria (scale, substitutability, interconnectedness).	HM Treasury designates CTPs (generally on regulator recommendations); the Bank of England, PRA and FCA then jointly oversee them.	**Firms:** Monitor designation lists in both jurisdictions; update third-party registers accordingly. **Providers:** Engage early with designation process; HM Treasury allows representations before designation.
Lead supervisors	ESAs through a Lead Overseer	FCA, PRA and Bank of England jointly	**Firms:** Understand which regulator leads oversight of your critical providers in each jurisdiction. **Providers:** Prepare for joint UK regulator engagement via the CCF; appoint central contact points.
Regulatory philosophy	Detailed, harmonised and prescriptive	Principles-based and outcomes-focused	**Firms:** DORA requires detailed compliance evidence; UK focuses on demonstrating outcomes. **Providers:** UK's principles-based approach offers flexibility but requires robust self-assessment capability.
Relationship with firms	Part of a wider DORA governance framework	Supplements existing UK operational resilience rules	**Firms:** UK firms can leverage existing operational resilience frameworks; EU requires DORA-specific governance. **Providers:** Understand how your services feed into firms' important business services (UK) or critical functions (EU).
Nature of obligations imposed	Direct supervisory oversight of the CTPP itself (Lead Overseer regime), plus a separate, mandatory minimum contractual code (Article 30) applying to *all* ICT third-party arrangements supporting critical or important functions, not just CTPPs.	Resilience obligations (self-assessments, scenario/resilience testing, incident reporting, skilled person reviews) imposed directly on the CTP by the regulators; no bespoke statutory contractual code layered on top of existing outsourcing rules.	**Firms:** Review Article 30 contractual requirements for EU; UK relies on existing outsourcing rules. **Providers:** UK CTPs face direct regulatory obligations (Fundamental Rules, eight Operational Requirements); prepare for self-assessments, scenario testing and incident playbooks.
Contractual mandate for firms	Firms must ensure contracts contain specified minimum terms (audit/access rights, sub-outsourcing transparency, exit strategies, service levels, cooperation with authorities, data location, termination triggers).	Firms rely on existing SYSC 8 outsourcing requirements and operational resilience rules (impact tolerances, mapping of important business services, exit planning) rather than a CTP-specific contractual template.	**Firms:** DORA mandates specific contractual terms; UK firms apply SYSC 8 and operational resilience rules. **Providers:** Expect EU clients to require Article 30-compliant contracts; UK clients focus on exit planning and service continuity.

Topic	EU DORA (CTPP)	UK CTP Regime	Key considerations
Consequence of provider non-compliance	If a CTPP fails to comply with Lead Overseer recommendations, financial entities must assess the risk and may be required to suspend or terminate the contractual arrangement (Article 42).	No equivalent statutory trigger compelling termination; firms manage this risk through their own exit planning and outsourcing risk frameworks.	**Firms:** EU requires risk assessment and potential termination if CTPP non-compliant; UK firms manage through exit frameworks. **Providers:** Non-compliance under DORA risks client terminations; UK enforcement includes censure and service restrictions but no fines.
Client/consumer-facing obligations	Financial entities must notify affected clients of major ICT-related incidents and maintain a Register of Information on third-party arrangements reportable to competent authorities.	Firms remain subject to existing operational resilience communication expectations and Consumer Duty obligations during service disruption, rather than any CTP-specific client notification regime.	**Firms:** DORA requires client notification of major ICT incidents; UK relies on Consumer Duty and existing communication expectations. **Providers:** Share incident information with firms to enable their compliance; UK CTPs must provide timely information to affected firms.
Testing and resilience	Detailed technical standards and supervisory expectations	Supervisory resilience testing and scenario exercises	**Firms:** Participate in CTP incident management playbook exercises; review CTP scenario testing results. **Providers:** Implement scenario testing within 12 months of designation; conduct biennial playbook exercises with representative firm samples.
Concentration risk	Embedded throughout DORA governance requirements	Considered principally from a financial stability perspective	**Firms:** Assess concentration risk across both regimes; map dependencies on designated providers. **Providers:** Understand that concentration is a key designation criterion; prepare for heightened scrutiny as market share grows.
Enforcement	Recommendations, inspections and periodic penalty payments	Supervisory directions and broader regulatory powers	**Firms:** Factor provider enforcement risk into third-party risk assessments. **Providers:** DORA allows periodic penalty payments; UK regime permits censure, service restrictions and conditions but no fines.
International coordination	ESAs coordinate across the EU and internationally	Formal cooperation with the ESAs under the UK-EU MoU	**Firms:** Leverage UK-EU MoU coordination for cross-border provider oversight. **Providers:** January 2026 MoU enables coordinated oversight; expect information sharing between UK regulators and ESAs.

Practical implications for cross-border activity

For institutions operating across both jurisdictions, the practical reality is unlikely to involve maintaining two entirely separate operational resilience frameworks. Instead, DORA will often establish the baseline governance architecture, while UK-specific requirements will need to be layered onto existing operational resilience arrangements. Nevertheless, firms should not assume that compliance with one regime automatically

satisfies the other. Differences remain in governance expectations, designation processes, supervisory engagement and regulatory reporting. Cross-border technology providers may likewise find themselves engaging simultaneously with multiple supervisory authorities, albeit under a growing framework of international cooperation.

Key compliance timelines

Firms operating across both jurisdictions should note the following key dates: DORA became applicable on 17 January 2025, and the UK CTP regulatory rules took effect from 1 January 2025. HM Treasury's CTP designations came into force on 13 July 2026. From their designation date, UK CTPs must submit an interim self-assessment within three months and maintain an incident management playbook within 12 months. Annual self-assessments are required thereafter, and biennial incident management playbook exercises must be conducted with a representative sample of firms.

Contractual considerations

- **Under DORA**, a regulated firm contracting with (or already using) a designated CTPP must ensure the underlying service agreement satisfies Article 30's minimum contractual provisions, which apply irrespective of designation but take on added significance once a provider is designated because the Lead Overseer's findings can directly affect the viability of the contract. Firms should build in: (i) full descriptions of the services and sub-outsourcing chain, including locations where data is processed and stored; (ii) unrestricted audit and access rights (including for competent authorities); (iii) clearly defined, measurable service levels; (iv) cooperation obligations enabling the provider to comply with Lead Overseer information requests, on-site inspections and recommendations; and (v) termination rights that are specifically triggered by supervisory findings against the CTPP (not merely ordinary breach). Firms should also insist on documented exit plans and transition assistance provisions that are realistic and testable, since DORA envisages that firms may need to exit a CTPP relationship on relatively short notice following adverse oversight findings.

- **Under the UK regime**, because the CTP designation itself does not create a parallel statutory contractual code, the firm's contractual leverage continues to derive from SYSC 8 (outsourcing) and the operational resilience rules. This means firms should still negotiate (1) step-in rights, (2) audit rights, (3) subcontracting notification/consent rights, (4) business continuity and (5) exit provisions — but these obligations exist because of the firm's own regulatory status, not because the counterparty has been designated a CTP. A practical consequence is that firms cannot assume a CTP designation automatically improves their contractual position, instead they must independently ensure the contract meets FCA/PRA expectations, since the CTP's own resilience obligations run to the regulators rather than to the firm as counterparty. Firms should nonetheless seek contractual cooperation clauses permitting the CTP to respond to regulator-mandated testing, information requests and skilled person reviews without breaching confidentiality, and should monitor whether the CTP's compliance with its direct regulatory obligations (e.g., resilience testing results) is shared with client firms, as this is not automatic.

Client-facing considerations

- **For firms operating under DORA**, client-facing obligations are more codified: firms must notify affected clients of major ICT-related incidents within prescribed timeframes, and should be prepared to explain how reliance on a CTPP affects continuity of service, particularly where the Lead Overseer's oversight activities (recommendations, fines for non-cooperation, or a request to suspend services) could disrupt the firm's ability to deliver to clients. Firms should also factor CTPP-related risk into their own disclosures and risk management communications to clients and ensure their Register of Information reporting to competent authorities accurately reflects the criticality of the relevant function.

- **For firms operating under the UK regime**, client-facing obligations flow primarily from existing operational resilience rules and the Consumer Duty rather than from the CTP designation itself. Firms must be able to demonstrate they can remain within impact tolerances for important business services even where a critical function is underpinned by a designated CTP and should be prepared to communicate proactively with clients in the event of disruption, consistent with existing expectations rather than any new CTP-specific notification duty. In practice, this means UK firms bear more of the burden of translating a CTP's regulatory resilience testing outcomes into client-facing risk management themselves, since there is no equivalent to DORA's built-in linkage between supervisory findings on the provider and mandatory client notification or contractual termination triggers.

Taken together, a firm dealing with an EU CTPP should expect a more structured, contractually enforceable framework with built-in linkages between supervisory oversight and termination/notification obligations, while a firm dealing with a UK CTP will need to rely more heavily on its own outsourcing governance, contractual drafting, and Consumer Duty-driven client communications, since the UK regime concentrates resilience obligations on the provider's relationship with regulators rather than mandating a parallel contractual code with client firms.

Dual-regulated entities and group considerations

For banking groups with operations in both the EU and UK, particular attention should be paid to providers designated under both regimes. Amazon Web Services, Google Cloud and Microsoft are designated as both EU CTPPs and UK CTPs. Firms should consider whether contractual terms negotiated to satisfy DORA's Article 30 requirements can also satisfy UK SYSC 8 expectations, or whether bespoke UK-specific provisions are required. In practice, DORA's more prescriptive contractual requirements will often establish a baseline that exceeds UK expectations, though firms should ensure exit planning, audit rights and incident notification provisions are appropriately tailored to each jurisdiction's regulatory expectations.

At group level, firms should assess whether a CTPP/CTP designation for services provided to one group entity creates indirect dependencies or concentration risks for other group entities. DORA's Register of Information requirements apply at entity level, but groups should consider maintaining a consolidated view of ICT third-party dependencies to support group-wide risk management. The UK regulators have not mandated a specific register format, but firms subject to both regimes may benefit from developing a unified third-party register that satisfies DORA's reporting requirements while supporting UK operational resilience obligations.

Exit planning and substitutability

Both regimes emphasise the importance of exit planning, but the practical challenges of exiting a major cloud provider should not be underestimated. Firms should ensure exit plans are realistic and testable, not merely theoretical. Key considerations include: (i) the time required to migrate critical workloads (which may extend to 18–24 months for complex deployments); (ii) whether alternative providers can deliver equivalent functionality; (iii) data portability and format compatibility; (iv) contractual provisions for transition assistance; and (v) the operational capacity to execute a migration while maintaining business continuity. Given that the same four providers dominate both the EU and UK markets, multi-cloud strategies may offer partial mitigation but do not eliminate concentration risk at the sector level.

Board and senior management responsibilities

Under both regimes, boards and senior management bear ultimate responsibility for third-party risk management. Under DORA, the management body must approve and periodically review the ICT risk management framework, including policies on the use of ICT third-party services. Senior management must ensure adequate resources for ICT risk management and maintain oversight of arrangements with CTPPs. Under the UK regime, boards should ensure that reliance on designated CTPs is factored into the firm's operational

resilience framework, including impact tolerance assessments for important business services. Firms subject to the Senior Managers and Certification Regime (SM&CR) should consider whether accountability for CTP-related risks is appropriately allocated within their management responsibilities maps.

UK-EU Memorandum of Understanding on CTP Oversight

In January 2026, the UK financial regulators signed and published a Memorandum of Understanding (**MoU**) with the ESAs (that is, the European Banking Authority (**EBA**), the European Securities and Markets Authority (**ESMA**) and the European Insurance and Occupational Pensions Authority (**EIOPA**)) on co-operation, exchange of information and co-ordination of oversight activities of critical ICT third-party service providers located in the EU and the UK.

The MoU lays down the principles and key areas for co-operation and exchange of information between the ESAs and the UK financial regulators as regards the oversight of EU CTPPs under DORA and UK CTPs under the UK CTP regime. This includes the co-ordination of oversight activities relating to EU CTPPs that own or use premises located in the UK for providing services to EU financial entities, and UK CTPs that own or use premises located in the EU for providing services to UK financial entities.

The MoU also aims to foster co-operation and exchange of information on ICT third party risk across different financial sectors, including in emergency situations. It aims to develop best practices for the review of ICT risk management practices and controls, mitigation measures and incident responses. This cooperation is intended to help the authorities manage risks to the stability of, or confidence in, their respective financial sectors.

Beyond comparison: A new regulatory perimeter?

The comparison between DORA and the UK's CTP regime is ultimately only part of the story. The more significant development is that both jurisdictions have reached the same strategic conclusion. Technology providers are no longer viewed merely as outsourced vendors. They are increasingly regarded as systemically important components of the financial system itself.

The UK government's decision to introduce the CTP oversight regime responded to conclusions and recommendations made by influential bodies in recent years. The Bank of England's Financial Policy Committee (**FPC**) concluded in June 2021 that "the increasing reliance on a small number of cloud service providers and other critical third parties could increase financial stability risks without greater direct regulatory oversight of the resilience of the services they provide." The Treasury Select Committee had earlier identified the risk of third-party providers becoming a potential source of concentration risk in its October 2019 report on IT failures in the financial services sector.

For decades, the concept of financial market infrastructure referred principally to payment systems, central counterparties, central securities depositories and settlement systems. Today, certain cloud providers and other critical ICT providers increasingly perform functions whose disruption could generate equally systemic consequences. The regulatory perimeter is therefore expanding beyond firms conducting regulated financial activities to include those whose resilience has become indispensable to financial stability. Furthermore, as firms' reliance on certain services provided by third parties increases, regulators may identify new potential CTPs. Certain third parties providing data and artificial intelligence (AI) or machine learning (ML) models could emerge as future potential CTPs as a result of the increasing use of these data and models in trading

systems. Investments by large technology companies (BigTechs like Google and Amazon) in emerging technologies such as quantum computing are likely to deepen their critical role in the financial system.

Outlook

The EU and UK have chosen different legislative architectures, but they are responding to the same structural transformation in the relationship between financial services and technology infrastructure. The limitations of the previous regulatory framework—where no single firm could monitor and manage risks stemming from a concentration in the provision of critical services by one third party to multiple firms outside its group—have driven both jurisdictions toward direct oversight of systemically important technology providers.

The more interesting question is no longer whether technology providers should be supervised. It is whether this represents the first step towards a new category of regulated financial infrastructure. As concentration risk, substitutability challenges and operational dependency continue to grow, future debates may increasingly extend beyond operational resilience into recovery planning, crisis management and perhaps even resolution-style frameworks for systemic technology providers. The regulators have already signalled that their horizon scanning may identify third parties that do not currently meet the criteria for designation but could do so in the future—particularly as AI, machine learning and quantum computing deepen the financial sector's reliance on a small number of technology providers.

For service providers to the financial sector, the introduction of the CTP regime marks many providers' first direct exposure to regulatory oversight by financial regulators. The regulators' requirements and expectations are agnostic about the location of CTPs, recognising that many CTPs provide services across international borders or to clients in multiple jurisdictions. This approach can help improve the efficiency and resilience of firms while reducing potential compliance costs compared to an approach that required CTPs to localise entities, infrastructure, personnel or services in particular jurisdictions.

The January 2026 Memorandum of Understanding between the UK financial regulators and the ESAs represents an important step toward managing the inherent cross-border nature of critical technology provision. As both regimes mature, the co-ordination of oversight activities—particularly in emergency situations and in relation to incident response—will be essential to managing systemic risks that do not respect jurisdictional boundaries.

In that sense, DORA and the UK's CTP regime may ultimately be remembered not as parallel operational resilience frameworks, but as the point at which financial regulation began to redefine the boundaries of the financial system itself—extending the regulatory perimeter beyond firms conducting regulated financial activities to encompass the digital infrastructure upon which modern finance depends.

About us

PwC Legal is assisting a number of financial services firms and market participants in forward planning for changes stemming from relevant related developments. We have assembled a multi-disciplinary and multi-jurisdictional team of sector experts to support clients navigate challenges and seize opportunities as well as to proactively engage with their market stakeholders and regulators.

Moreover, we have developed a number of RegTech and SupTech tools for supervised firms, including PwC Legal's Rule Scanner tool, backed by a trusted set of managed solutions from PwC Legal Business Solutions, allowing for horizon scanning and risk mapping of all legislative and regulatory developments as well as sanctions and fines from more than 2,500 legislative and regulatory policymakers and other industry voices in over 170 jurisdictions impacting financial services firms and their business.

Equally, in leveraging our Rule Scanner technology, we offer a further solution for clients to digitise financial services firms' relevant internal policies and procedures, create a comprehensive documentation inventory with an established documentation hierarchy and embedded glossary that has version control over a defined backward plus forward looking timeline to be able to ensure changes in one policy are carried through over to other policy and procedure documents, critical path dependencies are mapped and legislative and regulatory developments are flagged where these may require actions to be taken in such policies and procedures.

The PwC Legal Team behind Rule Scanner are proud recipients of ALM Law.com's coveted "2024 Disruptive Technology of the Year Award" and the "2025 Regulatory, Governance and Compliance Technology Award in 2025".

If you would like to discuss any of the developments mentioned above, or how they may affect your business more generally, please contact any of our key contacts or PwC Legal's RegCORE Team via de_regcore@pwc.com or our website.

Contact

Dr. Michael Huertas
Tel: +49 160 97375760
michael.huertas@pwc.com

Fabian Joshua Schmidt
Tel: +49 1514 1490437
fabian.joshua.schmidt@pwc.com

EU RegCORE Team
de_regcore@pwc.com

www.pwc.de