Regulators set out final rules for critical third parties to the UK financial sector

HOT TOPIC

November 2024

Highlights

The UK regulators set out the final rules for the critical third parties regime on 12 November 2024. This regulation brings into the regulators' perimeter third parties which provide services to firms for which failure or disruption could threaten the stability of, or confidence in, the UK financial system.

Contacts

Penny Flint
Partner
T: +44 (0) 7803 858309
E: penny.flint@pwc.com

James Houston
Partner
T: +44 (0) 7876 207850
E: james.r.houston@pwc.com

Tom Kohler
Director
T: +44 (0) 7940 510796
E: tom.kohler@pwc.com

Charles Rodger
Director
T: +44 (0) 7884 317642
E: charles.m.rodger@pwc.com

Conor MacManus
Director
T: +44 (0) 7718 979428
E: conor.macmanus@pwc.com

Hugo Rousseau
Manager
T: +44 (0) 7484 059376
E: hugo.rousseau@pwc.com

Summary

The BoE, PRA and FCA (the regulators) issued the final rules for the critical third parties regime on 12 November 2024. The package includes an overall policy statement (PS16/24), a supervisory statement (SS6/24) setting out the rules, a second supervisory statement (SS7/24) on Skilled Person reviews, the regulators' Memorandum of Understanding, and a document summarising their Approach to the Oversight of CTPs.

CTPs will be designated by HM Treasury (HMT) on the basis of the regulators' recommendation if they provide 'systemic third party services': those services provided to regulated financial services firms that, if disrupted, could threaten the stability of, or confidence in, the financial system.

The final rules are largely aligned with those proposed in the earlier Consultation Paper CP 26/23. However, the regulators have responded to feedback and have made changes to clarify, amend or moderate certain requirements and expectations.

Objective of the regime

The regime aims to reduce systemic concentration risks to the stability of the UK financial system by bringing systemic third party providers - the CTPs - into the scope of the regulators' supervisory oversight.

The regime is intended to increase the resilience of the UK financial system by strengthening the way CTPs identify, manage and respond to operational disruption whilst simultaneously reducing the impact of such disruption.

Designation and entities in scope

The regulators will advise HMT on designating entities as CTPs by assessing factors such as service materiality, market concentration, and systemic impact drivers, including substitutability. Regulators will periodically review whether a CTP still meets the designation criteria and will update HMT accordingly.

Entities that are already subject to authorisation, regulation, supervision and/or oversight by the PRA, Bank and/or the FCA with respect to the operational resilience of those services will not fall in scope of the regime.

Regulators are also unlikely to recommend a third party providing services to the UK financial system if its services are already regulated and overseen by other bodies with comparable outcomes to the CTP oversight regime, for example the UK National Infrastructure Resilience Framework.

Prior to designation, prospective CTPs will be invited to make formal representations within a reasonable period, typically three months. During this period, the CTPs can provide additional data and information to inform the final decision. HMT will consult with financial regulators and other relevant parties before making a final designation decision, which will be communicated to the CTPs and made public through Designation Regulations.

Services impacted

While HMT will be making the designation at an entity level, the regulators will identify which of the CTPs' services qualify as 'systemic third party services' (STPSs).

The term 'material service' from CP 26/23 has been replaced with 'systemic third-party service' to better reflect the systemic risk posed by these services and to avoid confusion with existing regulatory concepts.

Regulators may treat connected services from the same provider as a single STPS if their

combined disruption could threaten the UK financial system's stability or confidence. In such cases, regulatory rules apply to each individual service that supports the broader STPS.

SS6/24 contains a new section that explains how a CTP could impact the stability of, or confidence in, the financial system. The section details the structural features that make the financial system susceptible to either instability or a loss of confidence in the event of a 'CTP operational incident'. The regulators have expressed that it is 'vital' for every CTP to understand and familiarise themselves with the contents of this section, as well as apply it to the services they provide to customer firms. CTPs will need to consider how they will demonstrate that they have developed this understanding and embedded it into their culture and operating model.

The new rules will have implications for the shared responsibility model under which certain third-party services (notably cloud computing services) are currently provided. The model delineates responsibility for areas such as security and resilience between the provider and an individual customer. The regulators acknowledge that CTPs' duties under the oversight regime should generally correspond to their areas of responsibility within the shared responsibility model, but they stress that the model is not designed to address systemic risks. CTPs may find that the expectation on them to manage security and resilience is increased under the new rules, as the risk posed by the systemic nature of their services cannot be managed through responsibility sharing with individual customers alone.

Fundamental rules

CTPs will need to comply with six Fundamental Rules. These provide a general statement of a CTP's obligations that will underpin the oversight regime.

The Fundamental Rules cover:

1. Conducting business with integrity
2. Conducting business with skill, care, and diligence
3. Acting in a prudent manner
4. Establishing effective risk strategies and risk management
5. Organising and controlling affairs in a responsible and effective manner
6. Engaging with regulators in an open and cooperative manner, disclosing any relevant information.

In CP26/23, the regulators proposed that all six Fundamental Rules applied to all services provided by CTPs. In response to feedback, and in the interest of proportionality, rules 1-5 apply to STPSs only, whereas rule 6 applies across all services provided by CTPs. The regulators have maintained a broad scope for rule 6 to ensure that the regulators receive all information from CTPs that might be relevant to their oversight functions. CTPs may find that compliance with all six fundamental rules requires them to deliver entity-wide change.

The regulators have added examples to support the interpretation of some of these rules, including rules 3 and 6. For rule 6, matters the regulators would reasonably expect CTPs to provide notice of includes:

- changes to corporate or group structure
- changes to the STPS such as changes to the resources essential to the delivery of these services, including Key Nth Party Providers
- advance warning of incidents that are likely to develop into meeting the definition of a CTP Operational Incident on an imminent/short term basis.

Operational risk and resilience requirements (ORRRs)

The regulators have retained the eight ORRRs proposed in CP26/23, but have restated these in a more concise form, and made changes to clarify certain requirements. These rules are the core operational requirements for CTPs which cover:

1. Governance: CTPs must appoint a qualified employee or team to act as the central point of contact with the regulators. They must also establish clear roles and responsibilities at all staff levels involved in the delivery of STPSs.

2. Risk management: CTPs are required to develop and embed effective risk management processes that support their ability to deliver STPSs. Specific emphasis is placed on the need to manage dependency and supply chain risks as well as cyber and technology risks.

3. Dependency and supply chain risk management: the finalised requirements have been amended to direct focus onto Key Nth Party Providers. This includes the need to perform due diligence, obtain information on supply chain incidents to drive improved risk management and use an understanding of supply to chain to drive scenario testing. Contractual agreements with Key Nth Party Providers must be reviewed and updated in line with the CTP regime at the first appropriate contractual renewal or revision point following designation.

4. Technology and cyber resilience: Requirements target the need to ensure the resilience of technology that supports the delivery of an STPS. In practice, CTPs must establish robust processes that support the end-to-end management of technology and cyber risks.

5. Change management: CTPs must establish and embed a systematic approach to dealing with changes which is appropriately documented in policies, procedures and controls. This includes conducting thorough risk assessments, testing and validation before implementation. The requirements cover technology changes as well as changes to any other aspect supporting a STPS, such as people and processes.

6. Mapping: CTPs must identify and document all resources, including assets and technology, that support their STPSs. This must be done within 12 months of HMT designation, with continuous updates thereafter.

7. Incident management: CTPs are no longer required to develop a standalone, bespoke financial sector incident management playbook but must maintain and update documented plans and procedures to follow in the event of a CTP operational incident.

The requirement for CTP to set a maximum tolerable level of disruption no longer requires that these are compatible with impact tolerances set by customer firms for any important business services that are supported by systemic third party services.

8. Termination of Services: CTPs must establish measures to respond to the termination of their STPSs, including asset and data access, recovery, and return to firms. This includes developing practically actionable plans that can be shared with customer firms to support their own exit plan requirements.

Other requirements

The regulators provided further details which have been maintained from CP26/23 on their expectations for a number of areas including:

- **Information gathering**: CTPs must demonstrate their ability to comply with the proposed rules both annually and upon request.

- **Self-assessment**: Within three months of designation and annually thereafter, CTPs must submit a detailed self-assessment, keep referenced supporting documents for three years, and ensure assessments are comprehensive and transparent. The first self-assessment is now defined as an 'interim self-assessment'.

  Importantly, the regulators have required that the full annual self-assessments be shared with customer firms, albeit allowing for confidential or sensitive information to be redacted. This will provide more information to customer firms than was envisaged in CP 26/23, where a summarised self-assessment for customer firms was proposed.

- **Testing:** CTPs must regularly test for the continuity of their STPSs during severe disruptions, assess various adverse scenarios related to their risk profile, and test the effectiveness of incident management procedures on an ongoing basis, with potential additional tests to account for significant changes to how STPSs are delivered as and when required.

  Additional guidance has been included in SS6/24 to support CTPs to interpret 'severe but plausible' as well as select scenarios. Meeting the requirements on mapping and having a thorough understanding of Key Nth Party Providers will be critical in formulating insightful scenario testing.

- **Incident reporting and notifications**: CTPs will be required to inform regulators and customers about incidents impacting service, confidentiality, integrity, or asset availability. This includes an initial alert, ongoing updates, and a final incident notification. The phased approach to incident reporting has been retained, but the requirements for initial, intermediate, and final incident reports have been clarified and streamlined.

  CTPs will also have a broad obligation to notify the regulators of other relevant matters.

The international landscape

The regulators indicate the CTPs regime draws inspiration from and seeks to be consistent with global standards and guidance including of the FSB, the G7, the BCBS and the CPMI-IOSCO.

The regime is designed to be interoperable with similar non-UK regimes, such as the Digital Operational Resilience Act (DORA) in the EU and the Bank Service Company Act in the United States. However, this interoperability is maintained only to the extent that it does not conflict with or undermine the primary objective of ensuring the stability and confidence in the UK financial system.

The regulators expect to engage with international authorities as part of their oversight. To support this the regulators may request information from CTPs that has been provided to authorities in other jurisdictions and exchange information with authorities overseeing CTPs of mutual interest.

What does this mean for…

… third parties likely to become CTPs in the short term?

While most providers already have in place their own risk management resilience frameworks, this new regime will potentially require a significant uplift to ensure compliance with all of the regulators' expectations.

CTPs will be under the financial services regulators' oversight for the first time. CTPs will need to respond to regulators' questions and address their concerns, and could be subject to the regulators' broad range of powers (including the power to order Skilled Person reviews) should they fall short.

As a priority, entities likely to be designated should:

- Assess existing risk and resilience frameworks and their current control environment against the requirements.
- Develop an understanding of the services they provide that may become STPSs.
- Begin to draft an initial self-assessment that can be submitted within three months of designation.
- Prepare for oversight by the regulators, including developing an approach to regulatory engagement, that draws on good practice from currently regulated firms.

Entities should align their efforts with change programmes already underway to address requirements in other jurisdictions such as DORA.

There is also significant opportunity to leverage methodologies already developed for their financial services customers in response to these and other regulatory requirements; particularly those for UK operational resilience and TPRM under SS1/21 and SS2/21

… third parties unlikely to captured directly in the short/medium term?

Third-party providers not captured by the CTPs regime may benefit from aligning with the principal requirements of the regime, enhancing their ability to withstand disruptions and demonstrating a commitment to operational resilience.

… financial services firms?

The CTPs regime will not change the accountability of financial services firms for operational resilience, even when relying on third-party services. Firms will, however, gain access to new information from CTPs, including incident reports and self-assessments. Firms should review these against their existing assurance activities to identify opportunities for further alignment to support improved oversight.

Implementation and next steps

The CTPs' rules come into force on 1 January 2025. The obligations and requirements will apply to CTPs from the date on which designation takes effect.

The key next steps include the regulators providing recommendations to HMT of third-party providers meeting the criteria set out in the rules, and HMT deciding on prospective CTPs, which it will notify. These steps will take place on an ongoing basis, and we may see the first designations in H1 2025, accounting for the likely three-month representations period.

The regulators will also establish a joint CTPs Consultation and Coordination Forum which will coordinate the exercise of their CTPs functions.