Financial Services Regulatory Insights

Regulators propose oversight framework for critical third parties

AT A GLANCE

December 2023

What's new?

- The BoE, PRA, and FCA set out proposed requirements for critical third parties (CTPs) in a consultation paper (CP) published on 7 December 2023. The CP follows on a discussion paper (DP3/22) published by the regulators in July 2022.
- The regulators have released draft instruments and supervisory statements along with the CP, detailing the rules established in the CP and elaborating on the regulators' expectations.
- The regime aims to reduce risks to the UK financial sector stability posed by CTPs. Regulators are consulting on various requirements for CTPs, such as governance, risk management, resilience testing, and incident reporting.

What does this mean?

- The CP covers the same areas as DP3/22 but introduces new proposed rules with additional details on CTPs' minimum resilience standards.

Identification of CTPs

- A CTP is a third party service provider for whom failure in, or disruption to, the service they provide would risk the stability of, or confidence in, the UK financial system.
- The regulators will advise HMT on designating firms as CTP, assessing factors like service materiality, market concentration, and systemic impact drivers, including substitutability. Regulators will periodically review if a CTP still meets the designation criteria and update HMT.
- Firms already subject to an appropriate level of regulation and supervision/oversight (including in other sectors such as energy and telecommunications) are unlikely to be captured by the CTP regime.

Fundamental Rules

- The regulators have proposed six Fundamental Rules for CTPs, which will apply to all services offered to firms. These rules provide a general statement of a CTP's fundamental obligations to all services provided to firms.
- The Fundamental rules cover business conduct with integrity, skill, care, and diligence; prudent actions; effective risk strategies and management; responsible organisation and control of affairs; and open and co-operative engagement with the regulators.

Operational Risk and Resilience Requirements (ORRRs)

- The regulators revised the eight minimum resilience standards proposed in DP3/22 for CTPs regarding their material services.
- Key measures include:

1. **Governance:** Appointing a qualified employee to act as the central point of contact with the regulators. Establishing clear roles and responsibilities at all staff levels involved in the delivery of material services.
2. **Risk management:** Developing policies for risk identification, management, and review mechanisms. Continuous risk monitoring, including horizon scanning and threat intelligence use, is also expected.
3. **Dependency and supply chain risk management:** Performing due diligence, ongoing monitoring, transparency, and learning from disruptions and tests in risk and incident management processes.
4. **Technology and cyber resilience:** Implementing technology and cyber risk management and operational resilience

Contacts

Christopher Eaton
Advisory Director,
Head of Risk Assurance

T: +44 7797 900015
E: chris.eaton@pwc.com

Kevin Thompson
Advisory Senior Manager

T: +44 7797 915430
E: kevin.t.thompson@pwc.com

James Aldous-Granby
Advisory Manager

T: +44 7911 742052
E: james.aldous-granby@pwc.com

pwc

AT A GLANCE

December 2023

measures, as part of the broader compliance with risk management and testing requirements.

5. **Change management:** Deploying a systematic approach to dealing with changes. This includes conducting thorough risk assessments, documentation, testing, and verification before implementation.
6. **Mapping:** Identifying and documenting all resources, including assets and technology, and their internal and external connections for service delivery within 12 months of HMT designation, with continuous updates thereafter.
7. **Incident management:** Setting maximum disruption levels, maintaining and testing a financial sector incident management playbook. Engaging with established frameworks put in place by firms and authorities for coordinating responses to incidents.
8. **Termination of services:** Establishing to respond to the termination of CTPs' material services, including asset access, recovery, and return to firms.

Information gathering, self-assessment, testing and notification requirements

- In order to comply with the regime, the regulators also propose that CTPs comply with Information gathering, self-assessment, testing and notification requirements.
- **Information gathering:** CTPs will need to demonstrate its 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 documents for three years, and ensure assessments are comprehensive and transparent.
- **Testing:** CTPs need to regularly test for the continuity of their material services during severe disruptions, assess various adverse scenarios related to their risk profile, and test their financial sector incident management playbook annually, with potential additional tests as required. Regulators may mandate skilled person reviews for CTPs for various purposes, including resilience testing.
- **Notifications:** CTPs will be requested 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.

What do firms need to do?

- The CP proposals complement existing operational resilience requirements for financial firms. Firms need to remain compliant with their own obligations, including under SS1/21 and SS2/21, and the Senior Manager Regime.
- Firms should not assume that using a CTP is safer. This is made clear by the regulators which propose to prevent CTPs from unduly using their designation for marketing purposes.
- Potential CTPs should prepare for ongoing supervision by financial regulators. Key to this will be establishing clear governance frameworks and preparing for engagement with the regulators.
- CTPs whose head office is outside the UK will be required to nominate a legal person with authority to receive documents and notices from the regulators (including statutory notices under FSMA).
- Potential CTPs should assess proposed requirements and what steps are required to meet them. Critical elements will include risk management procedures, such as risk assessment, along with testing of the CTPs' resilience.
- Potential CTPs should evaluate cross-jurisdictional interoperability of similar regimes, including the EU's Digital Operational Resilience Act (DORA and the US's Bank Service Company Act (BSCA). Regulators propose collecting information shared with DORA and BSCA authorities and accepting compliant incident notifications.

Next steps

The consultation is open until 15 March 2024. The regulators also intend to publish a document establishing how they will carry their oversight roles in relation to CTPs in due course.

Contacts

Christopher Eaton
Advisory Director,
Head of Risk Assurance

T: +44 7797 900015
E: chris.eaton@pwc.com

Kevin Thompson
Advisory Senior Manager

T: +44 7797 915430
E: kevin.t.thompson@pwc.com

James Aldous-Granby
Advisory Manager

T: +44 7911 742052
E: james.aldous-granby@pwc.com