PATHLIGHT
ASSOCIATES LIMITED

CTP Regulatory Framework

February 2025

The UK is introducing a new regulatory framework for Critical Third Parties (CTPs) in the financial sector. Here's a summary of the changes:

What are CTPs?

CTPs are technology providers whose services are deemed essential to the functioning of the UK financial system. The failure of a CTP could cause systemic risk, hence the need for regulation.

What's changing?

- New oversight: The Financial Conduct Authority (FCA), Prudential Regulation Authority (PRA), and Bank of England will have direct oversight of designated CTPs.
- Rules and requirements: CTPs will need to comply with new rules, including:
  - Requirements broadly aligned with existing FCA/PRA regulations for financial institutions
    - Incident management and reporting requirements
    - Self-assessments and scenario-based testing
    - Setting a maximum tolerable level of disruption
- Focus on systemic risk: The regime specifically targets "systemic third-party services" that pose the greatest risk to the financial system.
- Shared responsibility: While CTPs are subject to new rules, financial firms are still accountable for their own operational resilience and third-party risk management.
- Increased transparency: Financial firms will have access to more information from CTPs, such as incident reports and self-assessments.

Key changes from draft rules

- Shared responsibility model: The final rules emphasize the shared responsibility between CTPs and their client firms.
- Focus on systemic services: Certain fundamental rules now apply only to "systemic third-party services."
- Flexibility in incident management: CTPs can use existing documented procedures instead of creating bespoke regulatory playbooks.

Timeline

January 1, 2025: The core framework and rules came into effect. This means the legal basis for the regime is in place.

Throughout 2025: The regulators (FCA, PRA, Bank of England) will proactively identify potential CTPs and recommend them to HM Treasury for designation.

From 2025 onwards: HM Treasury will formally designate CTPs. This is a key step, as the regulatory obligations only apply to designated CTPs.

Designation process

- Recommendation: Regulators recommend potential CTPs to HM Treasury.
- Notification: HM Treasury notifies the potential CTP, giving them an opportunity to make representations.
- Designation: HM Treasury issues a designation order, specifying the date the obligations come into force.
- Transition periods: There will be transition periods for some requirements to allow CTPs time to comply.
- Ongoing process: The designation of CTPs is an ongoing process, so new firms may be brought under the regime over time.
- No set timeline: There's no fixed schedule for designating specific CTPs. It's expected that the initial focus will be on major cloud providers and other significant technology firms.
- Early engagement: Even before formal designation, potential CTPs are encouraged to engage with the regulators and prepare for the new requirements.

Which Firm will be designated as CTP's?

It's still early days in the UK's CTP regime, and the official list of designated CTPs won't be published until later in 2025. However, based on the criteria and discussions so far, here are some likely examples of CTPs:

- Cloud Service Providers (CSPs):
  - Hyperscalers: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) - these dominate the market and many financial institutions rely heavily on their services.
  - Specialized Cloud Providers: Firms offering specific cloud solutions for financial services, like core banking platforms or trading systems.
- Data Providers:
  - Market Data Providers: Companies like Bloomberg, Refinitiv, and ICE Data Services provide essential market data feeds for trading and investment decisions.
  - Credit Rating Agencies: Firms like Moody's, S&P Global, and Fitch Ratings provide credit ratings that influence lending and investment decisions.
- Technology Infrastructure Providers:
  - Network Providers: Companies that provide critical network infrastructure and connectivity, such as BT, Vodafone, and Virgin Media.
  - Data Center Operators: Firms that operate the data centers housing critical systems and data for financial institutions.
- Payment Systems Providers:
  - Card Payment Processors: Companies like Visa, Mastercard, and American Express process a huge volume of card payments.
  - Payment Infrastructure Providers: Firms that operate the underlying infrastructure for payment systems, such as clearing houses and settlement systems.
- Software Providers:
  - Core Banking System Providers: Companies that provide the core banking systems used by many banks and building societies.
  - Trading Platform Providers: Firms that provide trading platforms for financial markets.
- Other Potential CTPs:

    - Artificial Intelligence (AI) providers: As AI becomes more prevalent in finance, providers of key AI models or data sets could be designated.
    - Cybersecurity providers: Firms providing essential cybersecurity services to the financial sector.

Important note: This is not an exhaustive list, and the final designation of CTPs will depend on the regulators' assessment of systemic risk. The regime is designed to be technology-neutral, so any provider of critical services, regardless of the specific technology used, could potentially be designated as a CTP.

Impact

- The new regime aims to strengthen the resilience of the UK financial system by ensuring that critical technology providers are subject to appropriate oversight.
- It will likely lead to increased compliance costs for CTPs and greater scrutiny of their operations.
- Financial firms will benefit from increased transparency and access to information, supporting their own risk management efforts.

Important notes

- The regime applies to CTPs regardless of where they are located.
- The regime complements, but does not replace, existing outsourcing and operational resilience rules for financial firms.
- Oversight of the CTPs is also part of DORA and the requirements in the UK are parallel to the EU. So, I think keeping an eye on the CTP designations in the EU might also give a sense of what's likely to happen in the UK.
- The requirements also link to identification of material outsourcing arrangements. The regulators will use the material outsourcing registers submitted to them for material outsourcing/third party arrangements to identify CTPs. For that reason, the FCA is consulting on making the submissions uniform and cover material third parties (CP24/28)

What CTPs need to do

- Meet FCA/PRA requirements: CTPs will need to comply with rules and standards broadly in line with those the FCA and PRA already apply to financial institutions. This includes things like:
    - Strong governance and risk management frameworks.
    - Robust financial resources.
    - Suitable and sufficient operational resilience.
- Focus on key areas: The regime emphasizes specific areas, including:
    - Dependency and supply chain management: Understanding and mitigating risks within their own supply chains.
    - Technology and cyber resilience: Protecting against cyberattacks and technology failures.
    - Change management: Managing changes to systems and services safely.
- Incident management: CTPs must have robust incident management and reporting procedures in place. This includes:
    - Promptly notifying relevant authorities of any major incidents.
    - Conducting thorough investigations and taking steps to prevent recurrence.

- Testing and self-assessment: CTPs need to conduct regular self-assessments and scenario-based testing to ensure their resilience.
- Provide information to clients: CTPs must be transparent and provide their clients with necessary information, such as incident reports and self-assessments.

What firms using CTPs need to do

- Maintain operational resilience: Firms are still ultimately responsible for their own operational resilience, even when using CTPs.
- Third-party risk management: Firms need to conduct thorough due diligence on CTPs and have robust risk management frameworks in place.
- Oversight and monitoring: Firms should actively monitor the performance of CTPs and their compliance with regulations.
- Contingency planning: Firms need to have contingency plans in place to deal with potential disruptions to CTP services.
- Communication and cooperation: Firms need to establish clear communication channels with CTPs and be prepared to cooperate in incident management.
- Reporting: Revise their reporting processes regarding material outsourcing arrangement
    - Identify materiality in alignment with regulatory expectations; and
    - Document sub-outsourcing arrangements, if applicable, to ensure they are also captured by the regulator while the CTPs are designated. For example, a foreign bank might be using a CTP through its HO.

Key takeaway

The CTP regime is about shared responsibility. Both CTPs and the firms that rely on them have a role to play in ensuring the resilience of the UK financial system. It's worth noting that the specific requirements for both CTPs and firms will depend on the nature of the services provided and the level of systemic risk involved.

Where to find the regulations:

- FCA Policy Statement PS24/16: This document sets out the final rules for the CTP regime.
- PRA Policy Statement PS6/24: This is the PRA's corresponding policy statement

Potential angles for an article/social media post:

The "Global Impact" Angle:

- Focus: Explore how the UK's CTP regime could influence regulations in other countries.
- Questions to explore:
    - Could this become a blueprint for international standards?
    - Will this lead to a global race to regulate critical technology providers?
    - How will this affect cross-border service provision?

The "Innovation vs. Regulation" Angle:

- Focus: Examine the balance between fostering innovation in financial technology and ensuring stability through regulation.
- Questions to explore:
    - Could the regime stifle innovation by imposing excessive burdens?

  - How can regulators ensure the framework remains adaptable to evolving technology?
  - Is there a risk of over-regulation stifling the dynamism of the fintech sector?

The "Cybersecurity Focus" Angle:

- Focus: Highlight the crucial role of CTPs in safeguarding the financial system from cyberattacks.
- Questions to explore:
  - How is the regime strengthening cybersecurity defenses in the financial sector?
  - Are the regulations sufficient to address the evolving cyber threat landscape?
  - What are the potential consequences of a cyberattack on a CTP?

The "Consumer Impact" Angle:

- Focus: Analyze how the CTP regime might ultimately affect consumers.
- Questions to explore:
  - Will this lead to increased security and reliability of financial services?
  - Could this result in higher costs for consumers?
  - How will this impact the availability and accessibility of financial services?

The "Future of Finance" Angle:

- Focus: Discuss how the CTP regime reflects the changing nature of finance and the growing reliance on technology.
- Questions to explore:
  - How is this reshaping the relationship between financial institutions and technology providers?
  - What are the long-term implications for the future of finance?
  - Will this lead to a more resilient and technologically advanced financial system?

Potential Pathlight Opportunities

- Advisory and independent review work for Firms working with CTPs - operational resilience / DORA
- Advisory work for CTPs
- Assurance work for CTPs on interim and annual self-assessments
- Skilled Person work for CTPs on behalf of the regulators