THIRD PARTY RESILIENCE AND THE IMPLICATIONS FOR THE FINANCIAL SECTOR IN THE UK

The Challenge

Organisations today heavily depend on external providers to operate successfully whether that be IT infrastructure, managed services, data and analytic providers or a host of new digital services which we couldn't even have imagined ten years ago.

With this heightened reliance comes potential for significant security and resilience risks.

Within complex digital supply chains, the failure of one link can trigger a cascading effect across other systems. Look no further than the recent CrowdStrike outage for proof. A seemingly minor software update brought down eight million computers, costing organisations millions in losses and interrupting businesses across the globe.

As a result of these increased digital dependencies, financial sector regulators have grown increasingly concerned about the impact a failure of a third party can have on the stability of banking and the broader financial sector.

Critical Third Party Regulation

This has been the key driver behind the recently released Critical Third Party (CTP) regulations (PS16/24) from the UK's Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA), although similar themes can be seen in the Digital Operational Resilience Act (DORA) from the European Union and its third party regime.

The UK regulations specifically address a growing concern about the concentration risk associated with certain providers in the financial sector. While the Treasury has yet to start the process of designating CTPs, we expect that these regulations will only target a small number of third parties whose failure has the potential to cause a major systemic issue for the UK.

For those third parties it brings an expectation that they will comply with a set of fundamental rules covering conducting business with integrity, due skill and diligence, acting in a prudent manner, having effective risk management systems, organising its affairs responsibly, and being open with the regulator.

It also brings specific requirements around operational resilience in areas of governance, risk management, supply chain management, technology and cyber resilience, mapping of services to underlying assets, incident management, and service termination.

The regulations also embed the concept of scenario testing and incident management playbook exercising, drawn from the broader Operational Resilience regulations – along with the idea of a self-assessment of the resilience state of the CTP which must be shared with the regulators and also (albeit allowing for redactions) with their financial sector customers and clients.

Incident reporting obligations also follow, not just to the regulators, but to any affected financial sector firms – and an expectation of engaging with sector collective incident response structures such as the Cross-Markets Operational Resilience Group (CMORG) sector response framework.

These new regulations come into force on the 1st January 2025, but at this stage await the designation of CTPs by the Treasury, which has its own process and consultation mechanisms. So while no firms will be impacted immediately, we can expect that cloud service providers along with the largest managed service and data providers can begin to see what awaits them if designated.

The Broader Supplier Community

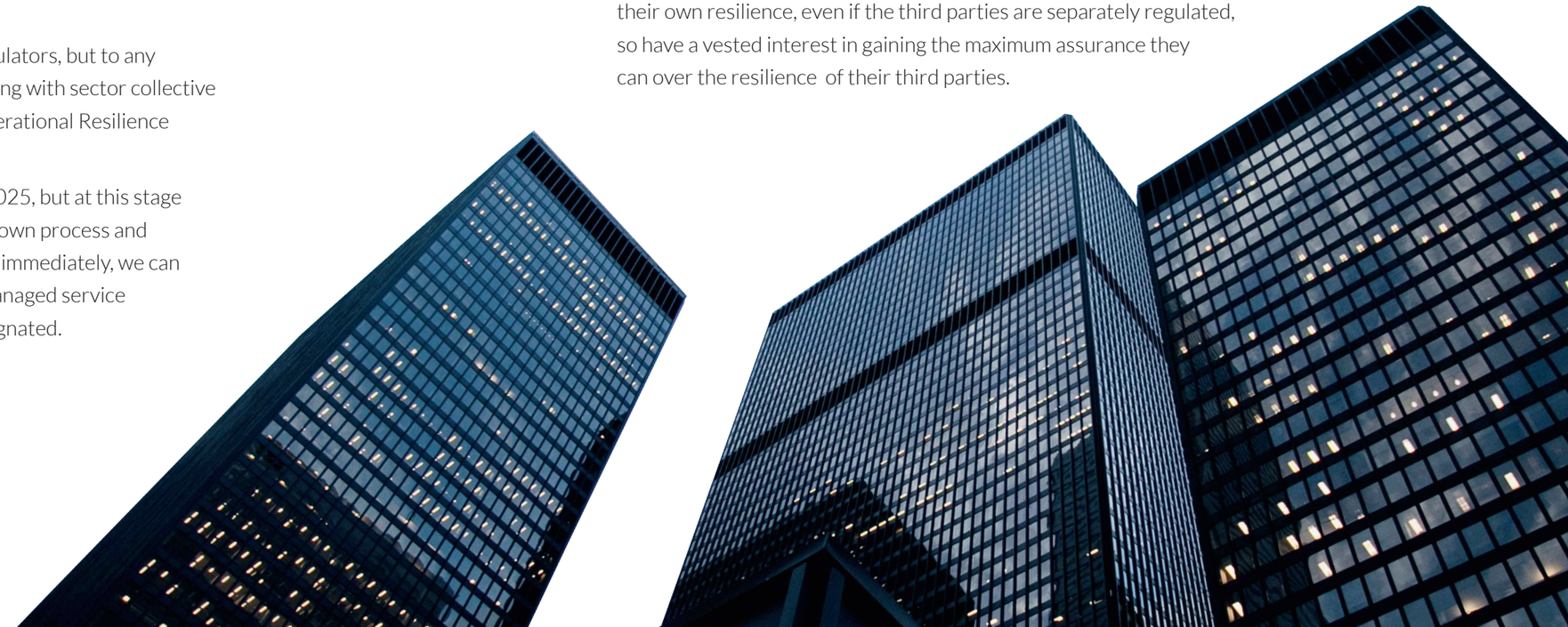
Looking beyond this small community there are many other third parties (hundreds potentially) whose failure may impact financial sector firms, but may not meet the demanding criteria of systemic importance set out in the CTP regulations.

This group of third parties may still cause an upstream client financial institution to fail to provide an important business service (IBS) to their customers, and indeed may even cause an outage of sufficient duration that the financial institution causes intolerable harm to its customers.

So the financial sector has been working to develop its expectations on that broader group of significant third parties. Those third parties won't be directly regulated under the CTP regime, but the banks and other financial firms who rely on them still need to be confident in the services they provide and their resilience.

CMORG has been developing guidance on just what may be expected of those third parties, and also responding to the concern that many of the third parties are being approached by their clients with very different asks over evidence of their resilience. With hundreds of regulated financial firms all asking similar, but subtly different, questions of their suppliers – there is potential for confusion and must wasted effort. This guidance was published in September (paper) and is essential reading for third parties who support the sector.

The guidance covers scenario testing, evidential requirements around resilience, alignment of contractual obligations on third parties, and also the scope for collaborative testing where a "test once use many" approach can be taken to reduce the test burden on third parties. Ultimately financial firms remain responsible for their own resilience, even if the third parties are separately regulated, so have a vested interest in gaining the maximum assurance they can over the resilience of their third parties.



The CMORG guidance covers five major aspects:

01 **Scenario Testing:** Supply chain partners should implement robust scenario testing frameworks, ensuring that their services can withstand severe but plausible disruptions. There is substantial experience across the sector now in how to undertake such testing and much that third parties can draw on as effective practice.

02 **Scenario Selection:** Selecting the right scenarios for testing is crucial. CMORG recommends using a scenario library, which includes a repository of severe but plausible scenarios, as a starting point. Scenarios should consider external threats, past incidents, and known vulnerabilities. They must also account for complicating factors, such as peak processing periods, concurrent system upgrades, or external events like extreme weather.

03 **Evidential Requirements:** Financial firms need clear, verifiable evidence that their third parties can respond to disruptive scenarios. This includes technical, organisational and contractual controls, such as backups and restore processes for critical data, recovery timelines and resilience governance structures.

04 **Contractual Obligations:** CMORG recommends embedding scenario testing obligations into contracts to ensure that third parties commit to supporting resilience requirements. Contracts should specify that third parties must conduct scenario tests and share relevant outcomes with financial firms. This not only facilitates transparency but also helps firms meet regulatory obligations.

05 **Community Testing:** Financial regulators and industry groups should promote community-wide testing initiatives to reduce duplicative efforts and foster collaboration across the sector. This approach involves multiple financial firms collaborating to sponsor tests that evaluate common third party services. For example, a cloud service provider might participate in a single test sponsored by several financial firms. This model enhances efficiency and could be particularly useful for commoditised services widely used across the sector.

By adopting these best practices, financial firms and third party providers can work together to meet the requirements of the Operational Resilience regulations, improve the stability of their services, while ensuring that critical services remain robust, even in the face of severe disruptions.

Looking forward

As we move into 2025 we can expect growing attention to be paid to third party resilience. We will see the initial CTP designations by the Treasury, but also the financial sector looking to operationalise the CMORG recommendations regarding third party resilience including the way ahead on collaborative testing. We may also see some more surprises as the Cyber Security and Resilience Bill progresses through Parliament in 2025, bringing its own regulatory requirements on managed service providers.