Digital operational resilience: the UK regulatory landscape

15 November 2024

Operational Resilience in the supply chain has become an undeniable priority for all financial service providers across the continent.

The significance of Operational Resilience has increased in parallel with developments in technology in the financial services sector. Its pivotal place as a risk to financial stability has been put further in the spotlight during recent cross border cyber incidents such as the worldwide IT outage caused by a defective update distributed by CrowdStrike and the outage at Swift, a global messaging service affecting wholesale payments.

Back in August 2024, the Bank of England ('**BoE**') published their Report on Operational Resilience on a Macroprudential Framework. This aimed to assist financial entities and the wider financial system to prevent and respond better to operational disruptions.

This has now been complemented by the Digital Rules on ICT Critical Providers published on 12 November by the BoE in collaboration with the Financial Conduct Authority ('**FCA**') and the Prudential Regulatory Authority ('**PRA**'). The Rules are aimed at levelling up cybersecurity and Operational Resilience to international standards.

1. **The BoE report: operational resilience in a macroprudential framework**

In March 2024, the BoE's Financial Policy Committee ('**FPC**') published a report exploring its attitude to Operational Resilience with the intention of highlighting how financial stability can be affected by operational risk.

This was further developed in the Report on Operational Resilience in a Macroprudential Framework, published on 27 August 2024 (the '**Report**').

Identifying macro vulnerabilities

The first step when considering macroprudential risks is, as highlighted in the Report, to take account of the level of Operational Resilience of financial services firms, Financial Market Infrastructures ('**FMIs**') and the wider financial system. The Report notes that the likelihood that an individual firm of FMI will experience an operational incident is determined by the number and extent of its (micro and macro) vulnerabilities.

The only possible way that these vulnerabilities can be centrally addressed is by putting in place robust operational risk management processes not just within the financial entities but also as regards their

critical service providers.

The Report states that macro vulnerabilities pose a greater risk of generating a domino effect which could threaten the stability of the financial system. It is for this reason that they are considered with particular care by the regulators.

System-Wide Resilience

The Report shows how Operational Resilience policies set by the regulators aim to narrow the gap between firm-level and system-wide Operational Resilience, highlighting how system-wide Operational Resilience is backed up by further system-wide policies and tools.

Relevant firms such as banks, building societies, insurers and FMIs are expected to:

a. recognise the vital services that are significant to financial stability when looking at their important business services;
b. consider how the wider financial system might be affected by deficiencies in their own Operational Resilience and implement clear processes to be followed when dealing with incidents as they attempt to increase their resilience; and
c. ensure that the impact of any disruption to the provision of essential business services does not go beyond certain tolerable levels.

The FPC also set out an expectation as to the time taken for critical payments to be made after an operational incident (known as the ‘FPC’s impact tolerance for critical payments’) and future new requirements to raise the resilience of material services provided by critical third parties to firms and FMIs.

The FPC have themselves taken steps to lessen systemic risks from operational issues by way of a program of work which includes stress tests to advance the financial system’s resilience to cyber-attacks.

System-wide resilience is to be supported by the cooperative attitude between the UK financial authorities and the wider financial sector through collaborative action and increased engagement within the sector.

Third Party Services Providers

The Report recognises the key role played by third party service providers to financial institutions.

Disturbances to the financial entities' services, or those of their third-party service providers, can directly impact the capability of the financial system to provide essential services. This can consequently affect multiple levels of the industry.

The Report makes clear that individual firms and FMIs' resilience may not be enough as standalone defences against system-level vulnerabilities. These vulnerabilities mean that operational incidents suffered by critical third parties serving financial entities, can cause contagion across the financial system. The result is that system-wide policies and tools are required alongside firm-level measures.

This point is further developed by the BoE in the PS16/24 Operation Resilience Rules considered below.

2. PS16/24 – Operational Resilience: Critical Third Parties to the UK Financial Sector

In recognition of the increasing reliance by financial entities on services provided by third parties, the impact of disruption to these services and potential threat to the financial stability and market integrity, the BoE, in collaboration with the PRA and the FCA (the '**Regulators**') have also issued Policy Statement PS16/24, titled "Operational Resilience: Critical Third Parties to the UK Financial Sector" on 12 November 2024 (the '**Rules**').

The Rules are set up on the foundational basis of the '*Overall Objective of the oversight regime for CTPs which is to manage risks to the stability of, or confidence in, the UK financial system that may arise due to a failure in, or disruption to, the services (either individually or, where more than one service is provided, taken together) that a CTP provides to 'firms*'.[1]

The Rules seek to harmonise various regulatory instruments across the Regulators, into a new Critical Third-Party ('**CTP**') Regime, comprising:

1. Critical Third Parties Instrument 2024
2. Critical Third Parties Emergency Provisions Instrument 2024
3. Supervisory statement 6/24 - Critical third parties to the UK financial sector
4. Supervisory statement 7/24 - Reports by skilled persons: Critical third parties
5. Policy statement 16/24 - Operational Resilience: Critical third parties to the UK financial sector
6. Approach to the oversight of critical third parties

The Rules, further explain in the Supervisory Statement,[2] outline the regulatory framework for oversight of CTPs and set out the Regulators' expectations of how a CTP should comply with the obligations placed on it under the Financial Services and Markets Act 2023 ('FSMA') and the Regulators' rules.

HM Treasury ('**HMT**') holds the authority to designate third-party service providers as CTPs[3]if their failure or disruption could threaten the stability or confidence in the UK financial system. Additional guidance will be provided by the regulators in respect of HMT's approach to designation of third-party service providers as CTP.

Pursuant to the Rules, CTPs are required to meet specific resilience standards, ensuring they can prevent, and deal with, operational disruptions arising primarily from Macro Vulnerabilities and Transmission Channels.

Macro vulnerabilities which can amplify the impact of an incident in ways which can affect financial stability include:

- *Concentration* - which arises directly as a result of arrangements between multiple firms and a third-party service provider, between a systemically important firm and a third party service provider, and/or indirectly through recurrent nth party[4] providers in the supply chains of multiple third party service providers.
- *Interconnectedness* - the inevitable large number of interconnections arise in an array of scenarios such as counterpart relationships. They increase the probability that an operational incident originating in one link of the financial system could have a knock-on impact on other links.

- *Correlation and common vulnerabilities* - when micro vulnerabilities become common, and they coexist across different entities.
- *Complexity and opacity* - in the case of interconnections and correlated common vulnerabilities, their complexity and opacity levels can augment the difficulty for financial entities to resist, respond to or recover from incidents.
- *The financial system's dependence on data* - If a CTP which has direct access to a financial entity's key data suffers a breach such as a cyber-attack, this could threaten the confidentiality, integrity, authenticity or availability of the firm's data.

Transmission Channels

In addition to macro vulnerabilities, the system is also threatened by Transmission Channels such as:

Contagion - when an initial operational disruption causes further (operational or financial) disruption elsewhere.

Loss of Confidence – when as a result of an operational incident, the financial system suffers a loss of confidence. Unlike the Contagion (which can potentially be mitigated), loss of confidence can be difficult to restore hence rendering a threat to financial stability.

Fundamental Rules

CTPs are expected to operate their business on the basis of six Fundamental Rules:

- Integrity;
- Due skill;
- Care and diligence;
- Acting in a prudent manner;
- Having effective risk strategies;
- Risk management systems;
- Organising and controlling their affairs responsibly and effectively;
- Dealing with each regulator appropriately in an open and cooperative way[5]

These Fundamental Rules should be exercised in a manner which is consistent with the Overall Objective.

Requirements

In addition to the Fundamental Rules, CTPs' obligations are set out across 8 overarching requirements:

1. Governance -
    1. Appoint central points of contact with the regulators who are overseeing them.
    2. Establish clear roles and responsibilities to staff who are essential to the delivery of a systemic third-party service
    3. Establish a clear approach to preventing, responding and adapting to any CTP operational incident
    4. Keep records of lessons earnt from previous incidents/testing exercises
    5. Notify regulators of key contacts, their contact details and any changes to this information

2. Risk Management
    1. Identify and monitor external and internal risks
    2. Develop and update risk management processes to effectively manage those risks
3. Dependency and Supply Risk Management
    1. Identify and manage any risk to its supply chain which could affect its ability to deliver a systemic third-party service
    2. Take reasonable steps and ensure that their Key Nth party providers are informed of the duties that apply to the CTP and cooperate with the CTP in meeting those duties.
4. Technology and Cyber Resilience
    1. Take reasonable steps to ensure the resilience of any technologies that deliver, maintain or support a systemic third-party service, including the development of comprehensive strategies and systems to adequately manage risks to technology; conduct regular testing of those strategies, processes and systems.
5. Change Management
    1. Develop systematic and effective policies, procedures and controls to deal with changes to systemic third party services, including changes to processes or technologies used to deliver, support, and maintain each systemic third party service it provides
6. Mapping
    1. Within 12 months from designation, identify and document:
        1. All resources, assets, supporting services and technology used to deliver, support, and maintain each systemic third-party service it provides
        2. Any internal and external interconnections and interdependencies between the resources
    2. Update these documents regularly
7. Incident Management
    1. Implement appropriate measures to respond and recover from CTP operational incidents
    2. Set up maximum tolerable levels of disruption to each systemic third-party service
    3. Maintain and operate an incident management playbook which sets out the plans and procedures to be followed in the event of a CTP operational incident
    4. Cooperate and coordinate with regulators and affected firms in response to CTP operational incidents, including through Collective Incident Response Frameworks.
8. Termination of Services
    1. Have in place appropriate measures to respond to a termination of any of its systemic third-party services by putting in place arrangements to support the effective and orderly termination of the service and provisions to ensure access to, recovery and return of any assets to each relevant firm to whom it provides the service.

The Rules also incorporate detailed guidance on self-assessment, testing and incident management playbook exercises.

UK v EU

Regulators across the EU are also preparing to implement the newly harmonised standards introduced by the Digital Operational Resilience Act ('**DORA**').

Effective January 2025, the key DORA obligations for financial entities in scope are structured around five pillars:

- Risk management framework
- ICT-related incident reporting
- Threat-led penetration testing
- Management of third-party ICT service providers
- Information sharing arrangements

The objective of the regulations is to enable financial entities operating in the EU to act in a coordinated and consistent manner in relation to cyber resilience in conjunction with their third-party ICT providers, including in the event of a significant cyber incident[6].

While both the EU and UK regimes share the same overall objective, there are distinct approaches across the legal frameworks.

In the UK, the focus is on Operational Resilience. the BoE emphasises system-wide vulnerabilities such as interconnectedness and concentration risks. Whereas in the EU, while there is consideration of a wide range of risks, DORA's focus remains on managing ICT-related risks and streamlining cybersecurity regulations for financial entities.

As regards their approach to critical service providers, another distinction lies in the requirement on an ICT provider to establish a subsidiary in the relevant region. Unlike DORA[7], in the UK, there is no requirement for a CTP whose head office is outside the UK to establish a UK subsidiary or branch under the CTP oversight regime[8].

However, there are undoubtedly areas in common. The UK Rules focus on CTPs, creating an oversight scheme. CTPs must meet specific resilience standards, conduct regular testing, and report incidents promptly. Meanwhile, DORA covers ICT service providers, introducing contractual standards, an oversight scheme and technical requirements too.

It is also clear that both regimes share the importance of proportionality[9] particularly in respect of third-party service providers. Regulators and financial entities in the EU are expected to take a proportionate approach to the application of the rules in DORA while in the UK, the Rules are clear on the obligation for regulators to consider proportionality in the exercise of their oversight functions to ensure that the rules do not become *unduly burdensome*[10].

Critically, they both agree on the importance of guiding financial entities and their supply chain towards a pre-agreed, robust, planned approach to incident management and the need to recognise Digital Operational Resilience as the ultimate priority on governance and policy development at an internal and external level, requiring active collaboration from all parties involved in the prudent management of systemic risks.

---

1. Operational Resilience: Critical third Parties to the UK Financial Sector, Supervisory Statement Section 1.3: Overall Objective, pg. 5.)
2. Supervisory statement on Operational Resilience: Critical Third Parties to the UK Financial Sector

3. A critical third party means an entity designated by HM Treasury in regulations made under s312L(1)FSMA. HM Treasury may designate an entity as a CTP only if it is satisfied that a failure in, or disruption to, services it provides to firms could threaten the stability of, or confidence in, the UK financial system (Operational Resilience: Critical Third Parties to the UK Financial Sector, Supervisory Statement section 2: Key terms, Key entities and persons, pg. 7.)

4. An nth party is defined as a service provider that is part of a third party service provider's ('TPSP's') supply chain and supports the ultimate delivery of a critical service by a TPSP to a bank or that has the ability to access sensitive or confidential bank information (Basel Committee on Banking Supervision, Consultative Document, Principles for the Sound Management of Third Party Risk, July 2024, pg. 4)

5. Operational Resilience: Critical Third Parties to the UK Financial Sector, Supervisory Statement Section 5: CTP Fundamental Rules, pg. 26

6. DORA, Article 2(1) (u)

7. Article 31(2) DORA refers to the establishment of a subsidiary of an ICT critical service provider in the EU.

8. Operational Resilience: Critical third Parties to the UK Financial Sector, Supervisory Statement, Section 4.12: No requirement to establish a UK Subsidiary or branch, pg. 22.)

9. See for EU, DORA Regulation (EU) 2022/2554, Article 4 and for the UK, Operational Resilience: Critical third Parties to the UK Financial Sector Supervisory Statement Sections 4.23 to 4.25: Proportionality pg. 14.)

10. Operational Resilience: Critical third Parties to the UK Financial Sector Supervisory Statement Sections 4.23: Proportionality pg. 14