Regulators publish consultation papers on "operational resilience" and outsourcing

December 16, 2019

Following a number of high-profile IT failures and data breaches in the financial services sector, a key priority for the Bank of England, Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) is to put in place a stronger regulatory framework to promote operational resilience of firms and financial market infrastructures.

The Discussion Paper "Building the UK Financial Sector's Operational Resilience", published in July 2018, set out an approach to operational resilience to start a dialogue with the financial services industry. On Thursday 5 December 2019 the supervisory authorities published a suite of documents which would embed that approach into policy. This includes a:

- shared policy summary published by the FCA, PRA and Bank of England;
- coordinated consultation papers published by the PRA (CP29/19) and FCA (CP19/32); and
- consultation paper published by the PRA on outsourcing and third party risk management (CP30/19), which is a key part of operational resilience. In part, this implements the EBA Outsourcing Guidelines which came into effect on 30 September 2019.

Consultation papers on operational resilience

The shared policy summary sets out a joint intention of the supervisory authorities to introduce "a stronger regulatory framework to promote operational resilience of firms and financial market infrastructures"[1].

The papers define operational resilience as the ability to "prevent, adapt, respond to, recover, and learn from operational disruptions"[2]. Importantly, it is acknowledged that such disruptions to daily operations will occur from time to time. The paper highlights the following key actions firms must take to reduce such disruption:

- **Important Business Services** – Firms should prioritise "important business services". "Business services" are those services that a firm provides to an external end user or participant. Business services will be "important" if their failure could cause an intolerable level of harm to consumers or market participants, harm to market integrity, or threaten policyholder protection, the safety and soundness of individual firms, or financial stability. The ability to make timely payments is specifically referenced in this context.
- **Impact Tolerances** – Firms should identify specific metrics for the maximum tolerable level of disruption for each service and should commit to remaining within these impact tolerances[3].
- **Scenario Testing** – Firms should carry out scenario testing to identify in which severe, but plausible, scenarios firms are able to remain within their impact tolerances.
- **Mapping** – Firms should have a comprehensive understanding and mapping of the systems and processes that

support their business services. Those who have previously performed similar exercises in connection with GDPR compliance programmes will know this can be a huge task in practice.

In practice, implementing these requirements will be a colossal task, requiring careful planning, governance and project management. Firms will need to ensure they take an integrated approach, engaging stakeholders from across the firm to identify risks to operational resilience, mitigating those risks where possible and planning responses where disruption occurs.

Sam Woods, CEO of the PRA, commented: “Operational resilience is a vital part of firms' safety and soundness, and has become an important priority for the PRA. This consultation marks the next stage of integrating operational resilience into our regulatory framework. Alongside this, our proposals on outsourcing and the cloud will steer firms to be resilient in their adoption of new technologies.”[4]

Consultation paper on outsourcing and third party risk management

The consultation paper published by the PRA on outsourcing and third party risk management (CP30/19) sets expectations on firms to maintain important business services when outsourcing or using third party providers. The paper reinforces the themes in the consultation papers relating to operational resilience in that firms should plan for, and minimise, disruption to services in a way that is communicated clearly to customers.

It acknowledges that the way in which firms are relying on third parties has evolved significantly over time due to factors such as technological developments (e.g. use of cloud) and lower operating costs. Although the paper recognises benefits of outsourcing and third parties, it identifies risks (e.g. the transfer of data and complex sub-outsourcing arrangements) that should be managed[5].

The paper sets out the following objectives[6]:

- complement the proposals set out in the operational resilience paper (CP29/19);
- “facilitate greater resilience and adoption of the cloud and other new technologies” as identified by the Bank of England in its response to the “Future of Finance” report;
- implement the European Banking Authority (EBA) “Guidelines on Outsourcing Arrangements”; and
- take into account the:
  - draft European Insurance and Occupational Pensions Authority (EIOPA) guidelines on outsourcing to cloud service providers; and
  - EBA guidelines on ICT and security risk management.

The consultation paper appends a draft supervisory statement that sets out the PRA's expectations on how firms should comply with regulatory requirements. The draft supervisory statement contains provisions dealing with:

- definitions of “outsourcing” and “third party” (chapter 2);
- proportionality (chapter 3);
- governance and record-keeping (chapter 4);

- pre-outsourcing phase (chapter 5);
- outsourcing agreements (chapter 6);
- data security (chapter 7);
- access, audit and information rights (chapter 8);
- sub-outsourcing (chapter 9); and
- business continuity and exit plans (chapter 10).

In particular, chapter 3 provides much needed guidance on how the proportionality principle applies to intra-group outsourcing, which has been one of the major challenges firms have encountered in implementing the EBA Outsourcing Guidelines.

Notably, the provisions have been drafted in a Brexit context so that "in the event that the UK leaves the EU with no implementation period in place, the PRA has assessed that the proposals would not need to be amended under the EU (Withdrawal) Act 2018"[7].

Conclusion

The consultations close to responses on 3 April 2020, and the supervisory authorities propose to publish their final policies in the second half of 2020 with implementation shortly after[8].

The supervisory authorities note that there has been a high level of engagement from firms on previous papers on this topic. Firms should ensure they respond to these consultations so that their voice is heard. In particular, the consultation paper on outsourcing and third party risk management (CP30/19) provides firms with an opportunity to address the challenges and uncertainties they have faced in implementing the EBA Outsourcing Guidelines.

Tristan Jonckheer is a partner in Dentons' Tier-1 ranked IT and Telecoms team in London. Michael Wainwright is a partner in Dentons' London-based Financial Services and Funds practice. This article was prepared with the assistance of Deepali Sharma, Trainee.

1. Foreword of the shared policy summary: see here↩
2. Para 1.8, CP29/19↩
3. Para 3, CP29/19↩
4. https://www.bankofengland.co.uk/news/2019/december/building-operational-resilience-impact-tolerances-for-import-business-services ↩
5. Para 1.8–1.14, CP 30/19↩
6. Para 1.1, CP30/19↩
7. Para 1.6, CP 30/19↩
8. Para 1.17, CP30/19↩

Your Key Contacts

Tristan Jonckheer
Partner, London
D +44 20 7246 7089
tristan.jonckheer@dentons.com

Michael Wainwright
Partner, London
D +44 20 7246 7735
M +44 7811 330 585

michael.wainwright@dentons.com