The challenges of demonstrating operational resilience: views from industry

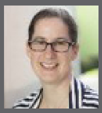
September 2020

With the UK consultation on operational resilience coming to an end on 1 October 2020 the window is closing to shape the final policy. The suite of consultation papers and draft policy statements published by the UK supervisory authorities[1] in December 2019 brought more detail about how the regulatory framework is intended to operate; but the papers inevitably brought more questions about how the concepts will work in practice. In August we saw the publication of a consultation paper on some operational resilience principles by the Basel Committee of Banking Supervision (BCBS) which have a lot of overlap with the direction set out in the UK.

UK supervisory authorities' definition of operational resilience: the ability of firms and FMIs and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions.

We brought together three leading industry practitioners on the topic of operational resilience and posed a set of challenging questions to them to hear how those responsible for developing their firm's resilience framework have started on their journey:

Kevin Thorne
RSA



Louise Gelling
UBS

Nicky Russell
HSBC

The paper is structured around the regulatory expectations of an operationally resilient firm, namely one which: prioritises the things that matter; sets clear standards for operational resilience; and invests to build resilience. For more background on the proposed regulatory approach to operational resilience you can read a summary in this **PwC hot topic**.

Prioritising the things that matter

To prioritise investment appropriately, a firm needs to understand the relative importance of the services it delivers where a disruption to the provision of the service could cause 'intolerable harm to consumers or market participants; harm market integrity; threaten policyholder protection; safety and soundness; or financial stability'. Those outcomes link to the objectives of the respective supervisory authorities. Firms also need to work out how the services are delivered by mapping out the various resources which are involved, which uncovers where the greatest dependencies lie.

> Practitioner: Fundamentally, (determining your important business services) should not be that complicated: consider where disruption would have the most material effect on end users.

> Practitioner: This is not about your ability to run a profitable business, it's about being able to provide the right outcomes to both customers and the market.

> Practitioner: The list of important business services shouldn't be static. We expect to review periodically to reflect changes in relative importance to customers, the firm and the market. This (exercise) is going to need strong change control.

PwC: On paper this sounds straight-forward enough but how do you know where to start when identifying important business services?

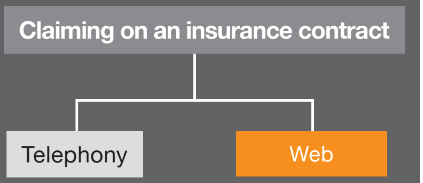
Practitioners: Firms should be able to work out quite easily which services[2] their end users rely on them for. The experience during this coronavirus ('COVID-19') pandemic may have given firms additional data on those services which are most important to end users and to the firms themselves.

Consider where disruption would have the most material effect on users. The art then comes in **defining services at the right level of granularity to support the setting of impact tolerances**. Ideally, firms should define their business services at a level which allows them to consider the different ways in which the end users need could be fulfilled, i.e. without specifying the channel. This will help firms to reflect multi-channel strategies as a way of building resilience into the design of the service.

Implications of defining business services by channel

The diagrams show that firms **defining business services agnostic of channel** can better represent the various alternative methods of delivering the service to stay within a stated impact tolerance.

For insurance the FCA suggests a business service could be 'claiming on an insurance contract'. While firms may be tempted to define it by their dominant channel, such as telephony, this would hide the use of other channels which could be used to divert traffic if telephony was disrupted, assuming the processes used different systems of course.

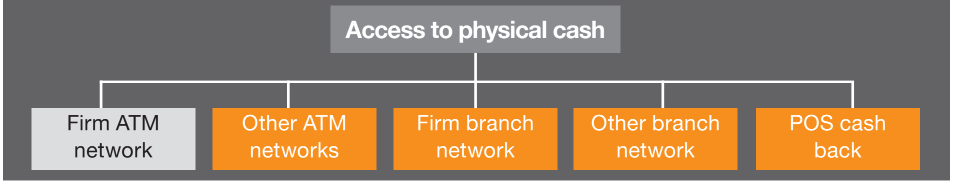


Claiming on an insurance contract

Telephony

Web

This example is even starker on a service such as 'access to physical cash'. Limiting this to a firm's own ATM network misses the wider range of alternative channels, and risks driving remediation activities which are potentially sub-optimal.



Access to physical cash

Firm ATM network

Other ATM networks

Firm branch network

Other branch network

POS cash back

Even if the supervisory authorities continue to shy away from defining a market-wide taxonomy of business services, there is merit in them guiding firms and industry bodies towards a common outcome to help themselves in compiling the system view. Ultimately, there is a finite number of things that end users, whether retail or institutional, want from firms.

The consultation papers have **refined the definition of business service to be about 'external end user or participant**', moving away from language on 'customers'. For firms delivering services to institutions (e.g. in corporate banking or investment management) there is a challenge around identifying the 'end user or participant' who may be once or twice removed from the firm, for example in investment management, or how important some activities are in providing liquidity and funding to other services offered to other end users. There are also some internal services, such as treasury, which may be common across most or all other important business services, where it may be beneficial to draw these out separately to manage complexity of the important business service maps.

[1] The Bank of England, Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA)

[2] While this paper focuses on the UK approach, it is worth noting that the BCBS principles on operational resilience (https://www.bis.org/bcbs/publ/d509.pdf) encourage firms to focus on their 'critical operations' rather than business services

> Practitioner: When working out how granular you need to map your service, go through several iterations of detail and stop when you can no longer think of any other support resources or when extra detail does not add any further incremental value.

PwC: Firms will be expected to have a map of how services are delivered end-to-end. Are you starting from scratch?

Practitioners: Firms will generally have some level of mapping in place to support business continuity planning or process improvement work – but these may not be aligned to the delivery of business services as now defined. Firms' experiences in their response to COVID-19 may have also enhanced their understanding of how services were being delivered.

There is a necessary exercise to **look at what exists already and use this to start building out the detailed picture of the service.** This will help to identify core resource dependencies which can form part of scenario testing, and to see possible alternative means of delivering the same outcome to the end user.

Working for a global institution can certainly make it more challenging to bring together a single, agreed view of how geographically separate resources actually support a service. **Start small by mapping one important business service**, as this will help to provide tangible material to have discussions with a wider set of stakeholders in due course, and will give you a consistent methodology to use for when you roll out to others.

Setting clear standards for operational resilience

To set clear standards, firms will define the maximum level of disruption that can be tolerated as a result of an operational incident. These are known as impact tolerances. The consultation papers provide additional details about how many to set, how to set them and how they differ from risk appetite. But the practical challenge of setting them remains, in looking through the eyes of consumers, the market and the firm itself. And the regulators have warned firms not to set them too high, such that they can always prove that they remain within them.

> PwC: firms should consider how technology can help them work through these concepts in a repeatable way driven by data. For instance, we can work with a firm to build a highly customisable Digital Twin of an important business service and enable the practitioners to look at the impacts of disruption over time, and to configure a range of scenarios to test the ability to remain within defined tolerance thresholds.

PwC: How do firms know where to set these tolerance thresholds?

Practitioners: This is the area with the least consensus across the industry but it should be quite straight-forward. Firms need to locate existing data to help measure the impact over time on end users, the firm and the market. Then estimate the maximum limits, and then validate them through a series of scenario tests. To understand the impact firms should look for data on their end users. Information from complaints, for example, gives a sense of what the impact is when services go wrong. Even firms serving corporate clients can analyse where business has been lost as a result of disrupted service.

Firms shouldn't feel confined by there being one set way to work towards impact tolerances. It can help to map a service before setting impact tolerances, to build an understanding of it, but similarly you could follow the same order as undertaking a business impact analysis (BIA), where you define the critical process first, then decide the RTO and RPO[3], and then identify supporting infrastructure. Firms should choose which approach works for them.

There is agreement around the industry tables that **the use of time to set an impact tolerance is only ever a proxy to measure the associated impact**. Saying a firm can tolerate an eight hour disruption to a service is only meaningful when considering what an eight hour disruption means in tangible terms (e.g. number of end users affected, what end users are unable to do, vulnerability of users).

Firms need to consider a range of adverse scenarios when working out the impact of disruption because this may manifest itself in different ways as illustrated in the examples below.

Practitioner examples of how disruption can vary based on the scenario use, for the service of 'accessing physical cash':

Scenario 1) the inability of a bank to match debit card data to PIN numbers could mean customers are not able to access their cash from any automated source provided by the bank or any other provider, potentially leading to customer harm if outside of branch opening hours.

Scenario 2) a disruption of a bank's own ATM network could mean customers are unable to withdraw cash from its ATMs, but they can use the branch channel or other ATM providers. This would put greater pressure on other market players to supply banknotes, without necessarily causing harm to consumers or having a notable impact on the bank itself.

Scenario 3) the hacking of a bank's ATM network resulting in fraudulent debit transactions could lead to large volumes of customers withdrawing their funds due to a loss of trust, negatively affecting its capital/liquidity position, though not having a long-term impact on customers (who are subsequently remediated).

The notion of dual-regulated firms having two impact tolerances has raised perhaps the most questions. Is it necessarily true that all important business services for dual-regulated firms will have impact tolerances for both FCA and PRA objectives? Based on analysis of incidents in the recent past, is it helpful if a firm determines an impact tolerance for safety and soundness at, say, a month? What behaviour change will this drive?

Some business services may be highly relevant to the FCA while having little safety and soundness or market impact from a PRA perspective. If a hypothetical firm identified ten important business services, perhaps seven of them would have two impact tolerances, two services may be relevant only for the FCA, and one service only for PRA. Tolerances for the PRA may be better defined at a firm level (i.e. business services taken in aggregate).

[3] Recovery Time Objectives/Recovery Point Objectives

Investing to build resilience

Firms need to test their ability to remain within their agreed standards of resilience and identify where vulnerabilities need to be addressed. This will help them to prioritise where to spend their finite budgets.

> “Practitioner: Ultimately, it's a simple exercise for the regulator to ask to see Board papers and ask how resilience was considered in making any decisions.

> “Practitioner: It's important for firms to balance both preventative and recovery capabilities – there is a danger that firms take the notion that 'failure is inevitable' too literally, and develop their recovery capability in isolation at the expense of preventative measures.

PwC: what do you think firms should be doing to ensure that current investment activity is improving operational resilience?

Practitioners: Much of the discussion in industry groups is on working out how the new concepts will be implemented in practice, like business services and impact tolerances. But of course, these are just a means to an end. **Ultimately what the regulators want to see is evidence that a firm has identified its vulnerabilities to important business services and has agreed a series of steps to improve their overall resilience.**

The CPs acknowledge that firms will already undertake testing programmes in areas such as business continuity, disaster recovery and crisis testing, and these will contribute to an overall view of resilience. However, for many firms it is a large step behind the nature of 'chaos testing' which the large technology firms are now adopting to build their own resilience.

The BCBS paper goes further than the UK in 'plumbing' its approach on operational resilience into existing frameworks. This includes drawing a strong link with recovery and resolution planning (RRP), expecting firms to leverage their completed work in that space and harmonise appropriately across the two. That said, where there are cases of jurisdictions adopting different definitions, such as in the use of 'critical operations' or 'important business services', multinational firms will face increased overheads to manage to differing expectations.

While working to the new operational resilience requirements will provide firms with data points to understand delivery of the business service and supporting resources, **they do not need to wait before changing the nature of conversations on resilience**. Firms can already embed this ethos of investing to build resilience now, even if it's a tactical approach until other work has been completed, for example: build in additional questions prior to agreeing capital investment; revisit existing spending plans to consider whether adjustments should be made such as where IT spend is based on 'upgrade-the-oldest-system' not the most important. **Too often, decision-making committees see information prepared in functional siloes**, but it is when proposals are worked through by a combination of functions that makes it more powerful. The success of this will depend on the approach of the individual who owns resilience at a senior level.

Going back to the definition of business services, by thinking about them at the right level you can consider what alternative methods exist to deliver it. **Ultimately, if there is a material disruption how will people get the service they need**. One way of increasing resilience in this case could be to ensure more end users are able to access different channels, and to signpost them.

The consultation papers outline the estimated costs of implementing the operational resilience policy, which are not insubstantial of themselves. But of course, **what firms are more interested in is the size of capital investment they may need to make** to address resilience concerns which is likely to be considerably more.

Closing remarks

There is no single right answer to becoming more operationally resilient. However, there is real benefit in the industry uniting behind a common way of doing things as it will ultimately improve the transparency of the resilience of the whole financial system.

This requires firms and the regulators to engage in an open dialogue, as we have seen here, to share evolving thinking and to agree good practice to be leveraged by the wider population of firms.

Contributors

Simon Chard
Partner

M: +44 (0)7740 241051
E: simon.c.chard@pwc.com

Stella Nunn
Director

M: +44 (0)7932 144627
E: stella.nunn@pwc.com

Adam Stage
Senior Manager

M: +44 (0)7483 422845
E: adam.stage@pwc.com

Sabrina Damian
Senior Associate

M: +44 (0)7841 804481
E: sabrina.damian@pwc.com

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

2020-09-20_RITM3721208