BANK OF ENGLAND

Speech

Resilience in a time of uncertainty

Speech given by

Nick Strange, Senior Technical Advisor, Supervisory Risk Specialists

OpRisk Europe

6 October 2020

I am grateful to Matt Lloyd, Jon Sepanski, Anne Wetherilt and Paul Williams for their assistance preparing this speech.

Good afternoon all, it's good to be back here at OpRisk Europe for a second year. And what a year it's been! Last year I said it's never been a better time to be an operational risk professional; little did I know how true that was about to become as Covid-19 presented one of the biggest operational risk challenges we've faced to date.

Background to the consultation paper

As a regulator, you might expect me to start with an update on the regulations. So I won't disappoint you. When the supervisory authorities (the Bank, PRA and FCA), published our first joint discussion paper (DP 01/18[1]) on Building the UK financial sector's operational resilience back in July 2018 we started a dialogue with the financial services industry. We define operational resilience as the ability of firms and the financial sector as a whole to prevent, adapt, respond to, recover, and learn from operational disruptions.

Our aim, then as now, was to build the resilience of the financial sector so that is better able to absorb operational shocks while continuing to provide what we have defined as important business services. We asked you all to assume these shocks would happen and to focus on your response and recovery capabilities – as case of "when, not if" disruption occurred.

A package of consultation documents followed towards the end of last year. Due to legal requirements governing the separate publication of policy for each of the authorities, it wasn't possible to publish just one consultation document and one statement of policy. For the PRA this was CP29/19[2] on Building operational resilience, but you can be assured that we are all still aligned in all the key aspects of the new proposed policy.

For completeness I should say that we issued a consultation paper on Outsourcing and third party risk management at the same time (CP 30/19[3]), but I'll not be touching on this today.
I ran through the detail of our then discussion paper on operational resilience at last year's conference, so I'll just briefly recap here. The proposed policy focuses on firms' ability to:

i. identify the important business services that they provide to their customers and to the UK economy more generally;

ii. set tolerances for disruption – 'impact tolerances' including time limits within which they will need to resume the delivery of these services; and

iii. invest to build resilience such that they can stay within these tolerances in severe but plausible scenarios.

Important business services

Avoiding disruption to particular systems is a contributing factor to operational resilience, but it is ultimately a business service that needs to be resilient – and needs to continue to be provided. We see a business services approach is an effective way to prioritise improvements to systems and processes. Looking at systems and processes on the basis of the business services they support may bring more transparency to, and improve the quality of, decision making, thereby improving operational resilience. Different standard setters or regulators may use different terminology, and I'll come back to this, but ultimately I believe we mean the same thing.

Impact tolerances and scenario testing

Firms should set their tolerances at the point at which operational disruption to important business services might pose a risk to financial stability, the firm's safety and soundness and (in the case of insurers) the appropriate degree of policyholder protection. Wary of getting into unhelpful discussions about probability

[1] https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf
[2] https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/building-operational-resilience-impact-tolerances-for-important-business-services.pdf
[3] https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/cp3019.pdf

we asked firms to assume these shocks would happen and to focus on their response and recovery capabilities – as case of “when, not if” disruption occurred. Probability is reintroduced in the UK model through the use of scenario testing.

We are also proposing specific requirements for boards to approve the important business services and the impact tolerances that have been set (outlined in the preceding chapters). We would also expect boards to satisfy themselves that their firm was meeting the requirements for having suitable strategies, processes and systems for identifying the important business services and setting the tolerances, and to perform mapping and testing

We originally set a deadline for responses to our operational resilience proposals of 3rd April 2020, but in recognition of the challenges posed by Covid-19 we extended this deadline to 1 October. We currently expect to publish our final policy in Q1 2021.

Early feedback from the operational resilience consultation

The level of engagement from financial sector firms and their service providers with both the discussion paper and the consultation paper was very impressive, showing that interest in this subject is far from waning.

As the consultation closed less than a week ago, it’s a bit early to give detailed feedback, but there are some high-level messages coming through from what we’ve seen so far:

- Respondents remain supportive of the UK supervisory authorities’ approach on operational resilience, particularly the focus on the resilience of important business services.

- They support what many have called a ‘paradigm shift’ for firms to assume disruption will occur, which encourages the development of response and recovery capabilities. However, they caution that this should not come at the cost of diverting attention away from improving preventative and detective measures.

- They want us to find effective ways to share what we see as good practice and to encourage firms towards consistency of application of the rules and guidance, as this will help in considering systemic threats.

- They want us to be proportionate in our application of new policy, keeping the proportionality that is already built into the CP.

- They want the UK supervisory authorities themselves to remain consistent both in principle and in practical implementation of the new operational resilience policy. For example: the degree of granularity that firms apply to identify important business services.

- They also call for consistency in two other respects, both of which I’ll return to:

    - Internationally, between different regulatory jurisdictions and global standard setters. This is particularly important to firms with a global footprint; and
    - Domestically, with other policies such as those related to recovery and resolution. This will help firms to implement strategic solutions which address common challenges.

We have also heard that firms are unsure how to assess the impact of disruption to their important business services on financial stability. As a central Bank we may be best positioned to consider the financial stability implications of certain operational outages. So in addition to firms setting their own tolerances, the FPC has indicated that it may set impact tolerances too and to this end announced in March 2019[4] that we would test an end-of-day tolerance for payments outages in a pilot cyber stress test. We undertook the test towards the

[4] https://www.bankofengland.co.uk/-/media/boe/files/financial-policy-summary-and-record/2019/march-2019.pdf

end of last year and will be going back to FPC later this year, following a delay due to Covid-19 disruption, to consider next steps for cyber stress testing.

Lessons from the pandemic

Let me say right upfront that we believe that the fundamentals of our proposed approach: important business services, impact tolerance, ensuring staying within tolerance, have stood the test of Covid-19. However, and as we expected given the timings, a number of respondents to the consultation have commented on the impact of the pandemic on their operational resilience so we will of course consider those before finalising our policy.

As we all know, Covid-19 continues to test the operational resilience and response capabilities of us as regulators and of the firms that we supervise. The nature and magnitude of operational risks have evolved as a result of the growing reliance on remote working arrangements.

We all, regulators and firms alike, focused first on maintaining the continuous delivery of important business services with reduced staff and very large increases in remote working.

- For many firms this has been more successful than they, or we, might have expected, largely due to the technical capabilities that are now available to us.

- But the huge increase in remote working has placed significant pressure on firms' IT systems which have needed to significantly scale up their capacity, and there have been practical problems too such as sourcing and configuring new IT equipment quickly and in large numbers.

- And at the same time firms have also had to deal with increasing demands for certain services (such as new loan requests or mortgage payment holidays).

No doubt productivity will have suffered, as staff juggle personal responsibilities such as child care with their work commitments, but overall the finance sector's response to Covid-19 is a relatively good news story. However, there is a real danger now that the pandemic is seen as an extreme test of operational resilience that proves that the financial sector is already operationally resilient. Does this mean "job done"?

We don't think so. There are characteristics of this event, extreme as it is, which made it easier for us all:

I. It evolved slowly – relatively speaking. We could see it coming; response time was measured in days, if not weeks. We had time to think. We had time to prepare and implement. And we had time to react in a controlled way, making it up as we go along – if you like. Like many of you, I've been 'practicing' for this for over 20 years by working from home from time to time.

II. It was prolonged – it has been with us for months now and will likely with us for many more months to come. This has given us time to understand and adapt to changing circumstances.

III. Finally and most importantly, it was symmetric in nature. That is to say that the threat has been broadly equal to everyone, everywhere, at the same time. Impacts may vary, based on local responses but essentially everyone was in the same boat. This gets you many things. Some level of goodwill or tolerance from your customers being one. But it also somewhat levels the playing field in terms of the response, i.e. if everyone's affected just as badly as me, then I'm not at an implicit disadvantage from a commercial risk perspective. And If I've got time to prepare, and react in a controlled and innovative way, then all the better.

But there are threats out there that will not be slow, prolonged and symmetric but precisely the opposite, fast, short-lived and asymmetric. Cyber is one such example but idiosyncratic operational failures or key third party failures will be fast, short lived and asymmetric.

Incidents with these characteristics, fast, short-lived and asymmetric, may rely on some of the same response and recovery capabilities but they will test an organisation's preparedness to the limit and in potentially different ways from that which Covid-19 has.

As firms rapidly changed their way of working to deliver their important business services, they have faced a changed operating environment and heightening of risks:

- First, the crisis has so far challenged the industry's thinking about business continuity in several ways. Some arrangements that were most likely planned (and tested) for shorter-term use will now be in place for much longer. So firms will need to be able to continue to offer important business services (such as trading and some retail operations) with high levels of remote working for a prolonged period of time. A clear focus on end point and network security is needed, with robust user authentication protocols.

- Many firms have also had to adjust their risk appetites and relax their controls, sanctioning ways of working they would not have accepted previously (such as remote recording of trading and enabling printing from home). This does increase fraud and insider trading risks, or the risk of confidential data leaks, but keeps important services running. Firms are now actively looking at how they can enhance their controls given the potential long-duration of the current arrangements. This necessitates clear remote access policies, detailed risk assessments of new solutions and real time security monitoring and patch management.

- At the same time, there is a question as to whether traditional approaches, based on remote disaster recovery sites, have now become obsolete, as working from home has (so far) proved to be a robust alternative solution. And if firms regularise forms of remote working (given the perceived benefits beyond the crisis) would that make them more resilient, or increase technology risk as a single point of failure?

- Relatedly, although the continuation of first line services has been a success, there has been reduced focus on second and third lines of defence. It is much harder for group risk and internal audit functions to operate remotely and still carry out detailed reviews with an intensive focus on control effectiveness. For example, some of the documentation that they would normally rely on may be inaccessible or just not there because procedures have changed.

- We note that some firms have understandably put IT change programmes on hold to allow them to concentrate resources on the short-term response to Covid-19, but that of course delays the resilience improvements that these programmes were meant to deliver. We are engaging through our normal supervisory channels to establish how plans are being reinstated for the most important of these projects

- Cyber risk too, has been increasing, although to some extent (so far) this is the dog that hasn't barked. Staff are now working much more on private networks, this increases the attack surface for cyber events. We've seen an increase in opportunistic cyber incidents, as phishing campaigns, which try to take advantage of people's natural concerns about Covid-19. User awareness campaigns are even more critical to maintaining cyber security.

- More significant cyber events have impacted third party providers. Which highlights the importance to firms of understanding the operational resilience of key third party suppliers, particularly if they are geographically distant. And exercising contractual rights to access, audit and obtain information from third-parties is even more challenging in the current environment.

So again we mustn't become complacent, it is more important than ever to make sure that appropriate controls are in place, cyber defences are strong, and that staff are reminded to exercise caution and be wary of phishing attempts.

I'll return now to the two high-level messages from feedback that I spoke about earlier on international and domestic policy harmonisation.

International regulatory harmonisation

Starting with international regulatory harmonisation. I should say that we invest a significant amount of time and resource engaging internationally and are active participants in most if not all of the many international forums bringing together regulators and firms around the world to discuss emerging operational resilience policy and practice. And we work bilaterally with key international partner regulators, forming strong relationships, with regular dialogue on operational resilience.

The Basel Committee of Banking Supervisors (BCBS) recently released its consultative document setting out 'Principles for Operational Resilience'[5]. They too seek to promote a principles-based approach to improving operational resilience. We are represented on the working group that produced this paper.

Looking at the both the UK and BCBS consultations, despite some differences in terminology, it is clear that we are aligned on the core principles:

a. A distinction between operational risk and operational resilience;

b. Operational resilience as an outcome, albeit defined in different ways;

c. Financial stability and safety & soundness lenses for operational resilience (consumers too for FCA);

d. Identification of what firms do that's important to both;

e. The concept of a risk or impact tolerance to define what might be acceptable (and not zero failure); and

f. The use of scenario testing to assure resilience.

We do need to manage firms' expectations though; perfect alignment of all details between regulatory bodies internationally is rare, but so long as the principles are aligned then firms should be able to work their way around local differences in implementation.

It's important that we supervisors play our part and cooperate to ensure that we respect and support each other's operational resilience concerns and priorities, particularly where supporting infrastructure reaches across boundaries.

Different jurisdictions will probably have different views on what they consider critical or important. This is not fragmentation; this is just accepting reality.

The key thing for international co-operation is that jurisdictions respect each other's judgement of what is critical and important. So that when the UK (or a UK firm) needs something to be operationally resilient and it uses US-based operational assets, we can work together effectively.

Policy harmonisation: Operational resilience and OCIR

The second area I said I would return to was domestic regulatory alignment.

Operational Continuity in Resolution (OCIR) and Operational Resilience are two policy frameworks delivering different outcomes but through the taxonomy of critical functions and important business services. I'm going to simplify things a bit to draw a high level comparison, but broadly…

OCIR policy aims to ensure that a *firm* continues operating *in stress and resolution* and ultimately continues delivering critical functions to the UK economy. This is an important aspect of a firm's resolvability:

[5] https://www.bis.org/bcbs/publ/d509.pdf

- The surest way to ensure continuity in resolution is for most or all of a firm's functions to continue throughout resolution, and hence, for all of the services supporting those functions to continue.

- For a successful post-resolution restructuring, in addition to critical functions, other business lines may need to continue to support the franchise and future viability of the firm.

- Ensuring continuity means that operational contracts need to be honoured (including payment obligations), staff employed and that a firm is ready to act if risks to continuity arise in resolution. It also means that a firm should ensure the delivery of the services it receives even through changes, for example, if a service provider has to be swapped for another as part of post-resolution restructuring.

Operational resilience policy on the other hand is designed to protect *some* of what the firm does *all of the time*, that is to say in stressed circumstances and in business-as-usual, to ensure the firm can continue to deliver important business services through operational disruptions.

- In the event of an operational shock, the firm must deliver its most time-critical, high impact services that have an external end user (important business services). Firms should identify services that could rapidly impact on financial stability, safety and soundness or policyholder protection and have contingency arrangements.

It is likely that a firm's important business services will be a part of that firm's critical functions. We therefore will expect firms to have a coherent narrative between what is 'Critical', or would support a firm's viability for OCIR, and what is 'Important' for important business services.

Irrespective of the terminology employed, boards and senior management should be aligned with us as regulators in wanting to know what aspects of their firms' businesses have the most impact on financial stability, their own business success and their customers' needs. So we don't expect to see completely different mapping regimes employed in a silo-based fashion. Work done to "map" and understand the interconnectivity of functions, business lines and services should be leveraged to meet the requirements of both OCIR and operational resilience policies.

Some thoughts on next steps

The relative success of working remotely means that for some staff the return to office can be slow, taking account of their own personal circumstances as well as business needs. As well as heeding government advice, triggers might also include reliance on public transport, school arrangements and the ability to ensure employees' health and safety in the office. Rotational working, staggered start/end of day times and split site working are all being considered. For the foreseeable future office occupancy rates will be much lower than normal.

I recently came across the 21/90 rule, often quoted by lifestyle gurus; "*it takes 21 days to build a habit and 90 days to build a lifestyle*". Well most people in the financial sector will have been working from home for double the 90 days and they're discovering that they quite like this new lifestyle! Firms are also starting to question what the new normal will look like. This has longer term implications the 'new normal' and for the control environment needed to mitigate the new risks we've discussed. The next session, 'Remote working and the new BAU', considers this interesting subject in more detail.

We will be looking to understand whether the firms who had made the most progress implementing our operational resilience policy proposals were able to respond best to this incident. There are some early indications that this is the case, as some firms were able to readily identify their key workers because they already had a good understanding of their most important business services.

As firms adapt to a new normal, that is the time to ensure that important business services are resilient by design rather than designed first with resilience as an afterthought. This is an opportunity to move to a new and higher level of resilience as you respond to Covid-19.