Operational resilience – outcomes in practice - speech by Lyndon Nelson

Given at UK Finance Operational Resilience Webinar

Published on 05 May 2021

Lyndon Nelson talks about how supervision of the financial sector in the UK has changed over the last 25 years.

Then he turns to recent policy on operational resilience. He says we have addressed some of the issues that firms raised in our consultation. These include:

- the relationship between Prudential Regulation Authority and Financial Conduct Authority policy
- the link to Basel, a set of international banking regulations

He goes on to look at the merits of outcome-based regulation of operational resilience.

Speech

It's late on Friday night. I'd been home for about an hour after a long week. The phone rings. My boss asks whether I could come in tomorrow as we are convening a small team to look into an emerging problem at a bank. The date is 24 February 1995, the bank is Barings.

I've actually been thinking a lot about Barings Bank recently and not for this speech, but partly at the request of our financial history team in the Bank of England (Bank), who collect first-hand accounts of events so that we can learn from those episodes. I'm not going to go through those lessons today, but I was struck in preparing my thoughts over 25 years later on Barings, just how profound the change to supervision since that collapse has been. For many Barings and the failures at Daiwa Bank were the inspirational sparks that began the first serious consideration of operational risk. Now of course many will point to earlier discussions in the Basel Committee and elsewhere, but there is no doubt that coincident with the failure of Barings the work of supervision changed. Focus shifted towards systems and controls and partly away from capital and liquidity. Now of course as we know from the Great Financial Crisis, ignoring capital and liquidity is not a good idea either.

Although I lack the clarity of hindsight looking forward, I do believe that the publication of our operational resilience final policy paper on 29 March[1] will provoke an equally profound change. If it does, we should congratulate ourselves that we made this change as part of a consultative policy making process and not in response to a crisis. I'm going to spend the first part of my remarks on our policy and the most common areas of feedback.

The Approach

Our policy approach is very close to the Discussion Paper we published in July 2018. As we have acknowledged our approach to this area of policy has been quite different. Most significantly, it is principle and outcome based and also it is the first policy to have been created in coordination with the four main UK financial regulators in this space: the Financial Policy Committee (FPC), the Financial Conduct Authority (FCA), the Bank as the supervisor of Financial Market Infrastructure and the supervisory authority within the Bank, and the Prudential Regulation Authority (PRA).

Coordinating the UK regulators where we could was an important policy goal. We heard from, and agreed with, industry contacts that the explosion of operational resilience and cyber standards risked shifting the effort of firms towards regulatory compliance and away from risk management. Furthermore industry added to our to-do list with a request from more than one location for harmonised global standards not just of regulation but also supervision. At the moment I may park that under the heading of a stretch goal, but I do think when we look at the latest Basel operational resilience text we are approaching a greater level of harmonisation than many thought was possible. Although considerable credit must go to our policy teams, I should acknowledge that the substantial positive engagement from the sector has significantly contributed to this outcome. The UK may therefore be able to claim to have one of the most harmonised regimes on operational resilience anywhere.

Nevertheless we continued to receive feedback from firms, which are jointly regulated by the PRA and FCA, that there were differences in language and definitions. Did this signal regulators looking for very different things? I would like to be very clear. Our joint intention is to operate the same regime, there are not supposed to be any hidden nuances in this policy, nor there be any differences in implementation. Work done for one regulator can and should be leveraged to meet the requirements of the other. Yes, we have had to use a different language, but only in order to fit in with the legal drafting norms of each regulator and to be sympathetic with the structure of their respective rulebooks.

The one point of difference, of course, remains that the PRA and FCA have different objectives and firms should obviously focus on those different objectives. Disruptions that may impact safety and soundness or financial stability could be different from those that may cause customer harm. If firms have back-up systems that protect the objectives of PRA and FCA, then that’s great – but expect each regulator to ask firms to demonstrate this.

As a Basel Committee member, I am very pleased with the Basel text on operational resilience. It has been too long to wait for the Committee to provide its views on this important issue, but as one would expect, what the Committee has produced is authoritative and thoughtful. We have, of course, had queries on the differences in language between our policy and the Basel text. Again the differences are largely due to the style and purpose of the documents. If one looks at the key features of both policies one finds:

- A clear distinction between operational risk and operational resilience;
- Operational resilience as an outcome;
- Financial stability and safety and soundness lenses for operational resilience (and customers too for FCA);
- An identification of what firm's do that is important;
- A concept of tolerance for disruption or impact tolerance to define what might be acceptable; and
- The use of scenario testing to assure resilience.

I feel confident that our approach will deliver the Basel principles for the UK.

I spent a good portion of my remarks at a UK Finance event on St Valentine's Day last year on outcome based regulation: its benefits and challenges. Although those days are a world and pandemic away, I will only mention briefly the importance of firms getting to grips with this approach. Firms frequently tell us that they want more outcome or principles based regulation as it works with the market and allows firms to find the most economic, efficient and effective way to meet requirements. Of course with no detailed prescription for firms to check their approach against, the challenge is that there is no ex-ante guarantee that you are meeting the requirements. This is obviously worrying for firms who fear the unjustified wrath of the regulator.

Suddenly the stifling straight-jacket of rules appears more attractive and we see an avalanche of requests for detailed guidance. Should we set up an operational resilience committee? How many important business services should we have? I could go on and on. I would ask those of you who are seeking this guidance to pause and reflect. In regulatory theory, what you are in effect asking for is a 'safe harbour'. If we do X then the regulator cannot touch us. Regulators typically do not like to offer safe harbours, it would be interesting to debate why. But that's not a debate for today. But I would suggest that even if safe harbours were on offer, I would argue to you that this should be of little comfort. Rigid and overly prescribed regimes are just what we need to avoid for a risk that is constantly evolving, and where key parts of it (such as cyber-risk) actually has a conscious opponent seeking to do harm. Having a safe harbour might reduce your cyber insurance premium, but it will not do much to reduce the probability that you suffer from an operational incident.

Another issue for respondents is the timelines for implementation. I've read a number of articles that say that the authorities are firing the starting gun and that this starts a twelve month countdown for implementation. It is true that operational resilience is a priority for the authorities as it is for firms. It is also true that within the regulators, there is little appetite for firms to delay implementation. But we know that we must be proportionate and that is what we will be. The word in the policy documents that is doing a lot of work here is "sophistication" - yes we are asking and expecting firms to have done quite a bit by 31 March 2022, but is it ultimately going to be everything that we expect firms to do? No. We understand and expect that tasks such as mapping and testing will evolve and will grow in sophistication over time. So by 31 March 2022, I would

expect that you will be able to set out a compelling gap analysis. You will know where your major shortcomings are and therefore which areas need more work.

Whilst on the subject of proportionality, I also wanted to flag that we have removed the requirement for all firms to have set impact tolerances with regard to financial stability. So for now only our largest firms will be asked to do this.

We have also said more about what I have previously described as the 'Family Tree'. That is how operational resilience relates to other operational concepts and in particular the PRA's Operational Continuity in Resolution policy[2]. The key point here is that firms have the latitude to implement our policies in a way that makes sense to them - if a set of operational assets are critical to the delivery of an important business service, mapping should be detailed and granular. If not, then such granularity would be the wrong thing to do. One of the benefits of not being prescriptive and following an outcomes based approach is that firms do not waste time. This way of thinking applies to other policies such as outsourcing and the use of third parties - we want firms to show us that they understand their risks and spend their energy and resources addressing them.

The Future

We acknowledge that there will be a number of challenges expected in the path ahead with the policy, and I wanted to touch on a few of these challenges in my remaining time.

Impact Tolerances

The first is impact tolerances and how these will play out between the different regulators. In truth it is too early to say because each regulator has yet to determine their final approach. The key for the PRA will be where the FPC and FCA decide to set their tolerances. For the FPC, it will raise the question to what extent PRA will need to interpolate the FPC's tolerance so that the contribution PRA regulated firms make to that tolerance are consistent with the outcome the FPC is seeking. For example, if the FPC determines a tolerance on payments, it is reasonable that we will take an end-to-end approach. What is likely to follow is that the functions of the payment system itself would need to be restored first, before providing access to direct members and then to indirect members and customers.

Business models

Another challenge is the shifting nature of business models. The Covid-19 pandemic has been largely well handled by the financial sector. It certainly has proved that a large number of business models can be resilient from the loss of premises and I know from the 4,000 branches of the Bank that suddenly appeared in March 2020 as our staff worked from home, that it is possible to be very effective. It certainly has not proved that the sector is immune to all shocks. Risks from the

pandemic will follow a different cadence to other types of risk and particularly a cyber-risk.

As we allow ourselves to think about a future living with the pandemic more under control, we can obviously think about the legacies good and bad from this terrible episode. I am sure like us you are thinking how you change your ways of working for the new normal. For many this has meant an acceleration of some technological roll-outs. We have seen a substantial increase in firms informing us of plans to advance digitisation strategies. This is clearly understandable as customers have demanded more of these services from the financial sector.

One real consequence of this change in pace is that plans to migrate functions to the Cloud that might have been stretched out over five years are now being spoken of in terms of a much shorter timeframe. At the same time we published our operational resilience policy[3] we also published our policy on Outsourcing and Third Party Risk Management.[4] The approaches are complimentary. We recognise the importance of the Cloud in enabling a scalable IT infrastructure that firms need to leverage the benefits of other technology such as Artificial Intelligence and Machine Learning or other analytical techniques. Moreover, if correctly configured, there are clear resilience benefits to financial institutions from cloud adoption.

There are also risks, of course. Some of these stem from the technological complexity, which is compounded by a shortage of relevant skilled resources in financial institutions. This can lead to shortcomings in the configuration of Cloud solutions and inadequate oversight. Moreover the public Cloud market is concentrated on a small number of large, unregulated providers whose services are increasingly critical to substitute, which raises questions of potential systemic risk. The challenge for regulation and regulators is to find an appropriate balance between these risks and enabling firms to leverage the benefits of Cloud solutions.

As I have spoken before a core principle in the financial regulation of financial institutions' outsourcing and third party dependencies (not just in the UK but around the world) is that financial institutions, their boards and senior management cannot outsource their ultimate accountability and responsibility. Nonetheless institutions can sometimes find it challenging to oversee effectively Cloud service providers. This can be due to the dominant position of the main Cloud service providers, which in turn can limit the ability of institutions to negotiate appropriate contractual safeguards and implement effective business continuity plans and cost strategies.

The operational resilience policy helps here. The identification of important business services, determining the maximum tolerance for disruption to those services and taking measures so that firms can remain within those tolerances under plausible scenarios, provides the right level of focus on cloud services and where substitutability is important.

We have also modernised our approach to outsourcing. Whilst the PRA, rightly in my view, has retained its technologically neutral position, we have addressed some of the specific nuances and challenges involved in outsourcing to a Cloud service provider. For example, there is a renewed

emphasis on data security, the management of sub-contractors and the supply chain (the latter having been a key cyber vulnerability in this past year) and the importance of testing robust business continuity and contingency plans. Given some of the contractual and practical difficulties that financial institutions may face in getting appropriate assurance from Cloud service providers, our updated policy also recognises a range of proportionate assurance mechanisms. For example, the use of what are known as 'pooled audits' where groups of firms work collaboratively to assess the control environment of a common service provider.

This collective action point is one I want to commend and expand upon further as my last remark today. Operational resilience is a very different risk when compared to financial resilience. Not least because of the size of the regulatory and central bank toolbox to deal with problems. In financial resilience we have a developed tool kit that can be extensive. Clearly the existence of the toolkit is not the same as the willingness to deploy it - the risks of morale hazard are well known. This contrasts with operational resilience. There is no bail out option if your firm is unable to function because of an operational incident. There is no operator of last resort function in Threadneedle Street. So we must find other tools to use. First of all firms will seek to be self-reliant, but for many (perhaps all) there will, I hope, be an increasing realisation that investment in collective action is a better way forward for many of the challenges that they face. The work of authorities such as CMORG (Cross Market Operational Resilience Group), FSCCC (Finance Sector Cyber Collaboration Centre) and FS-ISAC (Financial Services Information Sharing and Analysis Center) and other groups shows what can be done when the industry works together (often with the Authorities). As the co-chair of CMORG, I am perhaps a little biased, but I have been very pleased with the progress made and the work done so far.

So here we are 26 years on from that Friday night call. Quite a journey. Let's hope that if a similar call happens today or may be in a couple of years' time, the person answering will be able to enact their resilience plan and remain operational within a reasonable timeframe because of the work many listening today will have done.

I would like to thank Lee Elliot, Orlando Fernandez Ruiz, Amy Lee and Jon Sepanski for their assistance in preparing the remarks.

---

1. **Operational resilience**
2. **Operational continuity in resolution: Updates to the policy**
3. **Operational resilience**
4. **PS7/21 | CP30/19 Outsourcing and third party risk management**

Lyndon Nelson

Deputy CEO & Executive Director, Regulatory Operations and Supervisory Risk Specialists

Sign up for latest updates