Linklaters

Approaching the UK's operational resilience reforms: How to ensure you do it once and do it right – A speech by Julia Dixon and Pansy Wong at OpRisk Global

23 March 2021

- Financial institutions can set themselves up for a successful design and implementation of their Operational Resilience program by investing in governance, accountability and stakeholder engagement.
- Legal and compliance teams are crucial stakeholders in firms' programs to support the assessment and management of operational risks from a legal and regulatory perspective.
- Firms should look beyond day 1 implementation and prepare now for ongoing review and maintenance of the framework to ensure it stays up to date.

As partners in Linklaters' Financial Regulation Group, we are often instructed on programs like these once things go wrong: there has been a breakdown in the program; a weakness has been identified by an auditor or regulator; or a client has lodged a complaint about a failure to meet its needs. In looking at these issues, we see **common pitfalls and mistakes** that are made which can be very difficult to unpick or expensive to manage further down the line once the program or governance system is up and running. So today we are looking at the operational resilience reforms with a particular focus on the areas to look out for to avoid some of these pitfalls as you manage through your Operational Resilience program.

We will use the draft UK rules as our reference point but the principles we are going to talk through are equally applicable whatever flavour of global, or enterprise-wide, resilience program you are planning.

Setting yourself up for success

As the subject matter of our session says, our mantra is to "do it once and do it right" – which does involve more time and consideration at the outset but will pay dividends in the future. We know that some firms have gone some way down the path towards implementation already; others are waiting for the final rules before they kick off in earnest. Either way there is still time now to make sure you set yourself up for success. And of course, ideally you want to design and run your program in a way which ensures you do it once and do it right.

Governance

Governance is key. We have worked on many regulatory change and organisational transformation projects and in our experience there is a clear positive correlation between having the right governance plan in place from the get-go and successful delivery of the project. And this of course is especially hard for a project like operational resilience which will require input from stakeholders from across multiple areas of the business and multiple disciplines. Bringing them all together to **speak a common language** is very important.

And you need to think about governance in a few quite specific ways. There are a couple of things about the Operational Resilience program which are key to understand as the backdrop for why we are saying governance is so important in this case.

- Firstly, the rules themselves are intended to present a **cultural shift** in how firms prepare for and respond to operational incidents, and for this to be embedded in how those organisations operate, day to day. Whilst governance for any program is important, more often than not programs are about implementing a one-time fix or ensuring compliance with new regulations. Here, there is a need to ensure that the Operational Resilience program is integrated into the firm's existing governance structures so that it gets you into compliance and is fit for purpose in BAU. It is both a "change the bank" and "run the bank" program, if you like that terminology. It is really important, even as you are working through the early phases of your program, that you plan for and start to have engagement with the various governance bodies which the regulators will expect to understand and approve how the rules are put into practice in the organisation, and oversee the firm's resilience on an ongoing basis. Work cannot be conducted in isolation and presented as a "done deal" once the program team has done its work.
- The second thing to note is that, in our experience, many regulated firms who will be in scope for these rules do not operate their businesses or processes along lines that are specific to a legal entity. People think about activities or products more than entity structures, and these are often provided as global lines of business or services or support functions. This means, for example, that when you think of a service like "settlement", you do not necessarily think about it in the context of a single legal entity. Why does this matter? It is about **managing the inevitable complexity** in the most simple and harmonised but legally robust way.

When it comes to operational resilience, this is a subject where regulators across the globe are looking for firms to make change. Many firms are looking at operational resilience on a global or group-wide basis. The difficulty with this is that whilst the key objectives in say the US, the UK and EU regulations are pretty well-aligned, the actual requirements are not exactly the same, and they apply within a single jurisdiction and are applied at an entity level.

So, what does this mean in practice – in particular for your program governance? If you have your program governance reporting along functional global lines, you need to be careful that you get the right sign-off at a corporate level within the relevant jurisdictions. Taking the UK as an example, responsibility for the regime will rest with the board and other accountable Senior Managers. Given the individual accountability considerations, it will be important that the right jurisdictional and entity-level governance is put in place.

Accountability and stakeholder engagement

When it comes to accountability, it is really important to make sure that the right Senior Managers and other executives are **clear about their responsibilities** for compliance at the entity and jurisdictional level. If you are running resilience as a global program, it will be important to ensure that you have people locally who are responsible for thinking about the UK specific requirements and looking at the framework through a UK lens.

Anybody who has regulatory responsibility for the design or implementation of the resilience framework is going to need to be clear on precisely what their responsibility is. For example:

> If they are a Senior Manager, are those responsibilities reflected in their Statements of Responsibilities?

> Do they know how they fit into the overall framework?

> Can they speak fluently and comprehensively about the framework and their role in it?

With all this in mind, we think lawyers and compliance professionals should have a **seat at the table** for the design and build of the operational resilience program as their input into the governance and accountability aspects of this at the UK entity level will be vital, and the UK considerations might be difficult to pick out from a broader framework if a global program is put in place. Similar considerations arise when designing processes for data collation and escalation of management information, this needs to take into account any global program as well as the need for review and escalation locally, and to make sure that the correct information is provided to the correct persons. You would not wish, for example, to have information which is not specific to the UK entity being presented to the UK board. Similarly, any global responsibilities taken on by a UK executive will need to be clearly identified so it is clear which are subject of the UK regulatory regime and which fall outside or into another regime.

Documentation

We can hear a collective groan as a couple of lawyers talk about the need for documents – we are of course well-known for wanting to write things down. But this is a serious point. We see firms frequently trying to pull together an **audit trail** of what happened, or how a decision was made, often long after the fact and when people with direct knowledge of the matter have left the organisation. Firms frequently incur costs in employing external counsel or redirecting compliance and technology resources to review thousands of emails/meeting packs to try and find where or how a specific decision was made. Or they go through the pain of going back to the drawing board to try and reconstruct the thinking and justify the decision that has since been implemented. And the cost and irritation associated with having to repeat the work is not the only risk here. Often the trigger for an exercise of this type is a "red" audit and remediation point, a regulatory enquiry or request for the Chair of the Board to attest firm compliance etc. so there is organisational scrutiny and potential external risk exposure too.

When it comes to documentation it is not enough to have a record of the agenda that was set for the meeting. You need to think now:

> What are the decisions you actually need to make? And who needs to be involved with that?

> Can you track which decisions are to be made and by whom?

> Are they the right decision makers for the entity?

> Which of those decisions need to be flagged to the local entity board?

> How will you arrive at the inventory of your important business functions? What criteria will you use? And are you considering this in the context of the entity itself?

> Who agrees that the criteria are the right criteria?

There are lots of documents associated with this program and most of these will need input from legal and/or compliance teams. However, for these documents to represent effective conclusions and to provide the audit trail for how the end position reflected in these documents came about, really **clear documentation of decision-making and rationale used** is going to be critical to avoid expensive and time-consuming recreation of these later on, when someone – whether a regulator, a court, or an incoming Senior Manager or board member – wants to understand how a particular position was arrived at.

Similarly, and we will come onto this when we talk about the evergreen program, it is important to assist in making sure that any **future additions or amendments** to your framework are made using the same criteria and that this criteria itself can be reviewed and tested for currency periodically in the future. There is a danger perhaps that some operational resilience projects will be developed and implemented with minimal input from the Legal and Compliance team because this is seen as "an Ops thing" or a "tech thing", whilst we see many risks which could result in legal or regulatory risk if the framework is not set up correctly from the outset.

Legal and compliance issues to look out for

In this section we wanted to highlight a few points in the proposed UK rules, which, if not properly understood and assessed correctly at the outset, could snag the unwary in the future. These will hopefully highlight the need to have your legal and compliance teams as key stakeholders in your program so that the risks, and how they can be managed, are fully assessed from a legal and regulatory perspective.

The existing regulatory approach

Until the rules come into effect, the FCA and PRA in the UK review issues relating to operational resilience, broadly speaking, as **systems and controls issues** or through the more focused lens of the outsourcing requirements, for example. For the most part, these rules are broad in scope and will not be going away, of course. We have seen several examples of the FCA and PRA bringing enforcement action against firms under these rules. For example, Tesco Bank's cyber-attack failures in November 2018 (£16m fine) and Raphaels Bank's outsourcing failures in April 2019 (cumulative £2m fine), as well as other very public pronouncements about the adequacy of organisational systems and controls, such as the Slaughter and May Report into TSB's failed IT Migration in 2018.

When examining the adequacy of systems and controls and deciding whether to take enforcement action, a regulator will look at a firm's processes, decision-making and oversight and governance arrangements **with the benefit of hindsight**.

Thinking about an issue such as operational resilience which involves multiple interested stakeholders, overall regulatory responsibility for resilience is clearly an issue not only for the entity but also one/more Senior Managers will very likely be "on the hook" for the resilience framework design and all Senior Managers will be responsible for ensuring that the framework and ruleset is appropriately operationalised within their business or function. However, the multiplicity of interested parties and the enterprise-wide reach of the resilience agenda means pinpointing and maintaining operational responsibility for the program when it beds down in BAU more difficult.

Implementing resilience

This is what makes a program of this type hard and remediation challenging and expensive – it may not be clear where a breakdown occurred or why a process was not included in a review which may have prevented issues occurring. However, if done right, the framework which will be required under the operational resilience rules, should give a **clear roadmap** of the firm's important services, how they are supported and who is responsible for them. This means there will be an auditable record. This should make dealing with problems as and when they occur easier; the corollary of that is that it should also make bringing action against firms who fail far easier.

How you identify your "important business services" – broadly speaking those which could cause intolerable harm if they were not available to customers – is really important because a lot of the following rules rely on **getting this analysis right**. If you are coming up with a list comprising hundreds of important business services then you have probably got too many; equally if you do not have more than a dozen then, unless your business is very straightforward, you probably have too few. Whatever list you come up with, however, you will want to clearly document how you came up with the criteria for putting the service on the list as well as the criteria themselves.

The next piece in the puzzle is setting impact tolerance levels. This refers to setting the maximum level of disruption for each important business service. The FCA says that for their version of the rules this should include a "duration-based metric" ie how long a service can be out of action before it causes intolerable harm. This stage is crucial because the final requirement – and arguably the ultimate **aim of the whole regime** – is to stay within the tolerance levels that you have set for all your important business services.

The critical point to note here is that, under the UK rules as currently drafted, a failure to remain inside the impact tolerance level that the firm has set for itself results in a **regulatory rule breach**. The regulators do not need to prove any harm or negligence; a failure to meet your own tolerance level will be a breach. It is very like a speeding offence: if you drive at 35 miles an hour in a 30 mile an hour zone, you commit an offence, whatever the reason for doing so. We think it is important that firms consider both the important business services and the impact tolerance levels against this backdrop. This means that if you have a global program which identifies critical or important services and, say, one of those is not important in the context of your UK vehicle, you would want to make sure you are not including it in your UK program because if you include it and set a tolerance level for it you could be opening your entity up to potential liability, or undermining the design of your program, if you have not correctly assessed it against the UK entity's business.

For dual-regulated firms (ie those regulated by both the PRA and the FCA) there is an important distinction in their separate rules. The FCA rules are driven by an assessment of failures which could amount to customer harm, where the PRA rules are underpinned by an assessment of what could cause harm to financial services – and of course the two may not necessarily be the same. So dual-regulated firms need to be able to distinguish and **articulate where they are expecting to meet the different tests** or standards. Through both there will be a requirement to consider whether impact tolerance levels impact the viability or stability of the regulated entity itself, which again, is a different and distinguishable measurement.

Outsourcing

One other area we thought we would highlight for careful review is outsourced services – both intra-group and third party. In many organisations there will be several features of important business services which are provided by, or which rely on, services provided by other entities in the group, or third parties. Many organisations have inter-company service level agreements but, in our experience, in many cases, these are drafted in quite broad terms and have often been in place for many years. It will be important in the context of building a quality framework for identification and assessment of these services that a **critical review** is undertaken of the arrangements around these services.

When we think of operational resilience we often think about things like system outages or cyber-attacks, but data from a freedom of information request for the period 2018-May 2019 showed that the most frequent incidents reported to the FCA are third party failure, change management issues, hardware and software issues. We know from our own interaction with firms that the regulators are playing close attention to both outsourcing and third party service provider arrangements.

So, when you look at these services that support (or even comprise) your important business services, you will need to consider:

- > When was the due diligence carried out? Does this need upgrading?
- > Does the contract for the services need to be reviewed to make sure it adequately documents the service level you expect?
- > Does it provide for how you will carry out periodic assessments of the service level?
- > Does it cover all the services actually provided?

Similarly, when looking at intra group arrangements:

- > Is it clear who is responsible within the UK entity for procuring and assessing those services on an ongoing basis? (Hint: this is important for the Senior Managers Regime too).
- > Does the documentation clearly identify the services with enough granularity to be able to map them to the important business service in your operational resilience program?

Ultimately the rules (at least as currently drafted) will result in a **strict liability-style matrix** for your important business services and the impact tolerances set for them. Making sure that this is appropriate at the entity level, as well as making sure that it is clearly documented will be critical in ensuring that you are not trying to untangle things later on in the context of demonstrating compliance or dealing with any regulatory queries.

Making your program evergreen

We thought we would share what we have learned from other regulatory change programs we have worked on, or investigations work, when it comes to making your program evergreen form the start. That is to say: what you can do today to make your program easier to manage in the future, and to keep it up-to-date and accurate.

Day 1 v Day 2

We often see regulatory change programs focus on “go live” the date a regulation comes into effect, or the date a service is started, for example. We know from experience, that once a program has reached go-live, it becomes BAU, and **part of the day-to-day** of the organisation. This typically means that the team who have been focused on building out the program move on to something else, and the program governance ends. Where temporary or contracting staff have been engaged for the duration of the build, they are now reassigned or leave the organisation.

We know that this is a program which is going to become BAU. This means you need to think now about what you are going to do once your framework is established to ensure it continues to attract the appropriate attention and remains relevant and up to date.

There is a lot of crossover between the operational resilience framework which will be required by the rules and other programs. It is going to be really important to make sure – from a change management perspective – both that you draw upon the work that has already been done within your organisation (for example, we expect there may be useful knowhow that you hold internally from, eg your Senior Managers Regime, GDPR or even ring-fencing programs (if you operate in the retail banking space)) and that **changes in one program feed through to another**. For example, we expect organisations will need to align their recovery and resolution plans with operational resilience.

Changes in technology, new products and services; changes in the way functions which feed into those services operate (for example, newly automated systems); changes in outsourcing arrangements, reliance on a new third party or new technologies – **how are these changes captured and monitored** against the operational resilience framework on an ongoing basis to ensure that any changes to the framework are made in a timely manner?

Many of these changes will have their own change management processes – for example, new business approvals. This means that it is important to make sure there is an operating model, with appropriately assigned responsibilities, so that changes are given due consideration in the context of the operational resilience model, particularly with regard to the need to consider at the UK entity level. Similarly, the reverse is true. Say, for example, you have conducted enhanced due diligence on a third party supplier of a service which feeds into one of your important business services. You will want to make sure not only that the service levels remain consistent with the expectations under the operational resilience framework but also that any future changes to your outsourcing arrangements program do not adversely impact the standard of ongoing review required for the operational resilience framework.

It will also be important that boards and responsible Senior Managers receive appropriate periodic **management information**, incident reporting and so on, on an ongoing basis. To ensure they know what that information means and are well placed to oversee the real resilience of the business, senior management training will be important, as will refresher training and training for new Senior Managers.

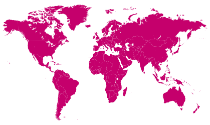
It will also be important for lessons learned to be incorporated into the program as well as documented as having been reviewed, assessed and factored into the framework – you will want to be able to point to these things. So it is really important at the outset to identify and engage with the teams and individuals who will be responsible for the ongoing governance of and upkeep of the framework from day 1; to know who is going to do it; and equally to know that sufficient resources are dedicated to this on an ongoing basis. For this reason, it is vital to adequately document this and ensure it is part of the discussion so it is not under-resourced and problems then occur: emerging risks are not adequately identified and addressed, lessons learned are not incorporated, changes are not considered fully. In some cases, it can be useful to do this with assistance from an **audit mindset** – thinking about how you would audit the framework in the future.

Hopefully this session will have given you a few things to look out for as you build out your program. Please do contact us if you have any questions.

Key contacts

Julia Dixon
Partner
Tel: +44 20 7456 4406
julia.dixon@linklaters.com

Pansy Wong
Partner
Tel: +44 20 7456 5018
pansy.wong@linklaters.com



Abu Dhabi | Amsterdam | Antwerp | Bangkok | Beijing | Berlin | Brisbane* | Brussels | Cape Town*** | Dubai | Düsseldorf
Frankfurt | Hamburg | Hanoi* | Ho Chi Minh City* | Hong Kong SAR | Jakarta** | Jeddah$^{\Delta}$ | Johannesburg*** | Lisbon | London
Luxembourg | Madrid | Melbourne* | Milan | Moscow | Munich | New York | Paris | Perth* | Port Moresby* | Riyadh$^{\Delta}$ | Rome
São Paulo | Seoul | Shanghai$^{\Delta\Delta}$ | Singapore | Stockholm | Sydney* | Tokyo | Warsaw | Washington, D.C.

** Office of integrated alliance partner Allens*
*** Office of formally associated firm Widyawan & Partners*
**** Office of collaborative alliance partner Webber Wentzel*
$^{\Delta}$ Office of Zamakhchary & Co. Linklaters in agreement with Zamakhchary & Co.
$^{\Delta\Delta}$ Linklaters Shanghai and Linklaters Zhao Sheng (joint operation office with Zhao Sheng Law Firm)

linklaters.com