KPMG

Operational resilience

Challenges ahead and how to avoid them

May 2021

kpmg.com/uk

For many firms, the newly-published operational resilience regulations set out a new way of looking at how their business operates and how it interacts with the broader insurance ecosystem. As firms engage with the new regime, a number of common challenges and pitfalls are emerging.

KPMG has already helped over 30 financial services firms in the UK market to build and strength their operational resilience capability in line with the new regulation. This paper sets out the top five challenges firms are facing in building their operational resilience capability, with some practical tips to help navigate the journey successfully.

Whether your firm is just starting out or is well down the road, this paper gives a great opportunity to learn from others' experience.

Operational resilience – the new regulations

The Operational Resilience policy statements were issued in March 2021 for financial services firms. As expected, firms have 12 months to build a resilience capability, conduct testing on important business services and agree investment around an implementation plan to mitigate any vulnerabilities. To put this in place you will be building on your firm's experience with COVID-19 as well as on existing operational risk, cyber, 3rd party and business continuity management capabilities.

Why are they challenging to implement?

Although this new regime builds on existing capabilities, there are some important aspects of the incoming regime that are new to many firms and that need careful consideration.

- End-to-end focus along important services – starting from the customer
- Impact tolerances, and what happens when you fail to meet them
- Stronger board ownership
- Increased focus on testing and also on people resilience.

These are new 'lenses' to many firms and are requiring a different mindset and focus to put into place.

The top 5 challenges and pitfalls

These are the top five challenges and pitfalls faced by or facing financial services firms as they build their operational resilience capability in line with the new regulations. The list of challenges come from our extensive experience of implementing operational resilience in over 30 financial services firms over the last three years. The accompanying practical tips have been successfully used in our own work with firms and by firms themselves.

The top 5 challenges and pitfalls

The top 5 challenges we are seeing in the market concern both short and mid-term implementation, and both internal and external components.

01

Defining your important business services How many, how granular, how to drive end-to-end accountability and manage across business units or countries

02

How to measure your firm's resilience defining resilience metrics, testing, data quality, MI dashboards and tooling/automation

03

3rd and 4th parties End-to-end resilience with ecosystem partners, influence over other parties, large supplier dependencies e.g. technology and cloud

04

Defining impact tolerances Defining intolerable harm, incorporating voice of customer

05

Embedding into BAU Investment prioritisation, keeping people engaged, real board ownership, service ownership, embedding into DNA of all staff

01. Defining your important business services

Context

- Business services are services that deliver an outcome to end users and customers.
- Important Business Services (IBS) are those services that, if disrupted, would cause the most harm to customers, the firm and/or the market.

Complexities

- The number of IBSs you have will be a function of the complexity of your firm. However, the more IBSs you define, the more complex your implementation will be. Choosing the appropriate number of IBSs is a decision for your firm.
- The end-to-end nature of IBSs mean they cross functional boundaries and silos. This perspective is often difficult to obtain and govern in the way financial services firms are run today.
- As the 'importance' of a service is a function of the potential harm that can be caused, it may differ by customer and by channel e.g. claim settlement may be more important to individual customers whereas mid-term adjustments may be more important for larger, dynamic risks.

"

We have made good progress in implementing the new regulations. It has been helpful to share resilience perspectives and approaches to defining business services with peers.

UK investment bank

Examples of specific challenges

1. Getting consistency and alignment where appropriate across different BUs or geographies which may involve different regulators.

Practical tip

Generate a long list of end-to-end services, then use structured, bought-in-to criteria to prioritise those that are really important. Not every regulator focusses on IBSs, so in a multi-country situation, allow BUs to vary according to local regulatory requirements.

2. Getting the organisation to understand the difference between the process taxonomy, organisation units and business services.

Practical tip

A great example is insurance claims. This may currently be managed as a set of processes, and as an organisational unit. The best way of showing how operational resilience would look at a claims IBS differently is to introduce it to the organisation using a managed pilot approach.

3. Whether to define important business services around activities that don't directly touch your customers and partners e.g. payroll or financial reporting. Firms are taking different approaches on this.

Practical tip

The important aspect here is to choose IBSs that are right for your firm. Whilst payroll is undoubtedly vital for the ongoing delivery of services any disruption here would generate end-user harm more slowly than is the case for some other services. You could also highlight its importance by mapping payroll systems and teams as assets underpinning other IBSs. Whichever way your firm goes on this question, the key is to have a good rationale behind the definition of your IBSs.

4. How to define and manage an IBS where your firm is not dealing directly with end customers. This could be where you feed into an intermediary who interfaces more directly with end customers.

Practical tip

In this case you should consider intermediaries as the users of the service, and consider the potential harm that could be caused to your firm, to the end customers and/or to the market if your business service in question failed to perform.

02. How to measure your firm's resilience

Context

— The best way to demonstrate to your stakeholders that operational resilience is understood is to get alignment on how to measure how resilient your firm currently is. This will help to manage and appropriately mitigate any gap to the vision and targets you set through your impact tolerances.

Complexities

— With financial resilience, you can quantify by how much balance sheet assets cover liabilities to customers, but how do you define and then quantify operational resilience?

— It's not enough to rely on scenario testing to test the resilience of your services. The regulators are clear that you need to understand the current asset condition under business-as-usual conditions before putting a scenario over the top.

— The resilience of your firm is only as good as its weakest link. The location and state of your weakest links will change over time with a changing external threat landscape, software and hardware updates, the state of buildings, people changes, data developments and outsourcing strategies. This is where having good resilience controls at an underlying asset level is important.

> **Operational resilience has helped us identify a number of synergies and opportunities for improvement across our business**
>
> UK retail bank

Examples of specific challenges

1. In order to get end-to-end resilience measures, you will need to harmonise across traditional functional and asset-based MI. These new measures can then be used to track progress towards the resilience targets your firm has set.

Practical tip

Define a summary board or exec-level dashboard up front to get alignment on how to measure and quantify resilience. Don't over-complicate it, use existing MI where appropriate and take time to understand how the measurement approach could improve over time.

2. Choosing a tool to use as a repository for the resilience framework components is important – this would hold your IBSs, mapping, impact tolerances, scenarios, attestations and remediation actions. There are a number of software platforms available – all have pros and cons.

Practical tip

Do the thinking up front about what automated and auditable tooling you may need in the mid-term. Even if you don't fully invest in tooling up front, the thinking will help re-work and re-design down the line.

3. IBS mapping to underlying assets can be a resource-intensive exercise, and most organisations change process flows and organisational roles and structures periodically as part of continuous improvement. If your resilience mapping does not keep up to date, the quality of your resilience monitoring will deteriorate.

Practical tip

Whether your firm has high process discipline or whether it runs more free form, it is much easier to keep your resilience framework aligned with operational changes if the first line owns that alignment. A tool that is easy for all to use will help keep ownership in the first line.

4. Your firm will probably rely on information from many internal systems and from manual attestations to power your resilience dashboard. This can result in many versions of the truth, and in subjective opinions as to asset vulnerabilities. It can be a lengthy and costly journey to fully automate all resilience controls.

Practical tip

When improving and automating your resilience monitoring, cleanse your data sources to identify single-sources-of-truth before investing in automated links between your resilience tool and underlying systems.

03. 3rd and 4th parties

Context

- The regulator is looking for firms to monitor outsourced service providers involved in the provision of important business services, including their ability to stay within impact tolerances.
- This will include identifying where your 3rd parties utilise outsourced service providers and what controls they have in place.
- Where those IBSs involve 3rd parties and/or captive and intragroup suppliers, the firm will need to demonstrate how it will minimise harm if these other entities are disrupted.

Complexities

- Your 3rd parties may rely on 4th or 5th parties to perform services for your firm with whom you have no relationship and no contractual rights – you may not even be aware.
- These external parties may not be regulated by the FCA, PRA or Bank of England and so may not appreciate the importance and challenges of these new financial services regulations.
- If outside the UK, these external or captive parties may be subject to parallel but not identical operational resilience regulatory regimes.
- The extent to which you can get suppliers to change how they work to support your firm's resilience may be restricted by existing legal contracts.
- In the short-term it is not always easy to find substitutions for third-party services or to bring them in house.

Examples of specific challenges

1. Some firms are already working hard to configure supplier relationships towards improving resilience. However including 4th and 5th parties is new ground for many firms and for the suppliers themselves.

Practical tip

The operational resilience lens can be used to improve the interface with other parties so that both parties benefit. Increased transparency, better data exchange, more joined-up testing and recovery management can help to improve efficiency and to strengthen the mid-long term relationships.

Practical tip

Where you interface with other regulated entities, be on the front foot when it comes to defining IBSs and impact tolerances – otherwise your partner firms may define them for you.

2. Persuading external suppliers to expend resource in joint end-to-end testing is not always easy. This is particularly difficult when different firms are asking for different testing scenarios and timetables.

3. Exposure to large supplier dependence e.g. software houses or cloud providers. Many FS firms will rely on 3rd party technology providers who service many firms. This can mean that, on your own, you cannot get these 3rd parties to work towards improving your firm's resilience. Similarly, where you work with 3rd parties to whom your business is not material e.g. many global cloud providers, it may not be realistic to expect the 3rd party to change their operations to support your firm's resilience.

Practical tip

For suppliers who work with multiple firms, we suggest they find a common way of working with their partner firms on testing and on improving end-to-end resilience to avoid having to run endless crisis- management scenarios that could otherwise consume considerable amounts of their resource.

Practical tip

Where you are reliant on a 3rd party who is unlikely to make any changes on your account, it is important to have practical workarounds where possible in the event of a disruption. Access to any data shared between organisations is often the key.

> **I'm going to look for my material suppliers who support IBS to better evidence their resilience. Why shouldn't all my key suppliers do the same?**
> Large UK general insurer

04. Defining impact tolerances

Context

— An impact tolerance describes the maximum level of disruption that external beneficiaries will tolerate in terms of harm caused or before the firm's viability is threatened.

— An impact tolerance is defined at an IBS level and is unique to an individual firm and its customer base.

— By setting impact tolerances, firms should then be able to carry out scenario testing in order to assess the firm's ability to recover within those tolerances. This will identify vulnerabilities and remediation actions and better understand as to where to prioritise investment.

Complexities

— Impact tolerances can only ever be subjective and aggregate measures that serve as a crude approximations of external harm.

— They need to be defined assuming a scenario-agnostic disruption to an IBS will occur at the worst possible time, volume and context. They also need to be proportionate, based on the firm's profile and its impact on consumers and market integrity.

— The regulators are not expecting firms to be able to withstand any possible disruption with no loss in service. In this way, there are some scenarios in which your firm cannot avoid harming others, although the regulators will expect your firm to minimise that harm and to recover expediently. Your impact tolerances should be set with this in mind, on the basis that they will be breached in some situations. This adds complexity in determining the right tolerance levels.

Examples of specific challenges

1. Defining absolute levels of intolerable harm for stakeholders and relating those back to measurable performance of IBSs will be an imprecise and subjective exercise. The greatest value of an impact tolerance resides in its use as a planning tool to guide and prioritise a firm's allocation of scarce resource to effectively build resilience across a portfolio of business services.

Practical tip

Avoid over-analysing impact tolerance definition. Your tolerances are likely to change as you learn more about your firm's ability to recover from disruptions and as you improve your resilience. The key is that your impact tolerances are the result of a well thought-through, logical process, based on the reality of your business.

2. Your firm will have customer satisfaction, partner feedback and complaint data which will help indicate how those who depend on your services may feel about reduced service following a disruption. The challenge is to collect enough evidential data, and to use and combine these data sets in a way that is consistent with the logic you have defined.

Practical tip

Focus on relative rather than absolute calibration of impact tolerances, and on ongoing longer-term calibration over reporting cycles.

3. Setting time-based impact tolerances is easier as they can relate back to traditional, asset-based recovery time objectives (RTO), but it is harder to set volume-based tolerances on the basis of harm caused.

Practical tip

Initial calibration of tolerances should be informed by historical events both internal and external. Use impact data from previous BCM scenario testing and live events as well as voice of the customer to assess where it is feasible and appropriate to set impact tolerances. RTOs will be an input but will not be the answer. When defining tolerances, keep the concept of flexible workarounds in mind. Where a disruption affects a service, you may be able to recover performance within the impact tolerance with practical workarounds.

“

For us, resilience is not just about investing in processes but also streamlining them. We expect to see process efficiency savings. Resilience is everyone's job

Global composite insurer

05. Embedding resilience into BAU

Context

— Firms are typically approaching this new regime with a change programme mindset to build the operational resilience capability, with a view to then transitioning into a BAU operational activity.

— Your new capability will build on existing business continuity management, Cyber and Risk Management frameworks including business impact assessments and orderly wind-down scenarios and plans.

Complexities

— Whilst there are a number of overlaps with existing frameworks and capabilities, operational resilience brings new requirements and looks at firms in a new, cross-functional, end-to-end way. This will require new skills and capabilities, and will need education and culture change to embed properly.

The new focus on taking an end-to-end perspective has been beneficial to the firm, but to make it work has required a new mindset in some key roles.

Financial market infrastructure provider

Examples of specific challenges

1. Your Board needs regular updates and visibility in this area, but ensuring that operational resilience governance is appropriately owned at Board level is a difference from more traditional BCM and disaster recovery (DR) ownership. The Head of Resilience must build the firm's capability, but the Board must demonstrate they are doing their job too.

Practical tip

Whilst Boards typically have deep experience, awareness that they may not have all the tools and knowledge for this new way of looking at their firm is the first step. Education will play a role, and it may help to use experienced 3rd party advisors to inject some challenge.

2. Business service ownership on an end-to-end basis will be new to most firms. Finding the right role and modus operandi for business service owners alongside business unit and asset owners will need careful design and culture change.

Practical tip

Design the operating model up front, including business unit and asset owners in those conversations to gain engagement. A strong Operational Resilience Committee can set the tone for how the organisation should evolve.

3. Many recovery professionals have a traditional BCM mindset. If you want your firm to improve its resilience by behaving and responding differently, it may require different skills in your central team to support this transformation.

Practical tip

Consider hiring from outside financial services, or from financial services institutions who are ahead in this space.

4 Investment prioritisation for resilience mitigation activities is difficult when competing with other initiatives that have more obvious P&L benefits. It is a challenge some firms are already concerned about. Regulators will expect to see a fully-funded mitigation plan. Board and executives may need a different way of comparing investment opportunities to be sure to allocate limited resources appropriately.

Practical tip

To aid in investment prioritisation decisions, consider the additional benefits that operational resilience mitigations could bring to give your firm competitive advantage – e.g. cost reduction, more effective 3rd party interfaces, more reliable data and technology and potentially a stronger customer proposition.

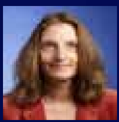
5 Once you have implemented the new framework and capability, keeping people engaged and preventing operational resilience from becoming yet another compliance tick-box exercise is not easy. The final frontier is embedding an operational resilience mindset, principles and skills into the day to day lives of all your teams and suppliers.

Practical tip

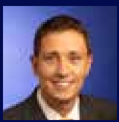
Take the time to set a strong and clear vision for what operational resilience will mean for your firm and communicate this effectively to all staff. In addition, build operational resilience into every initiative in the change stack.

Contacts

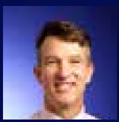
Andrew Husband
Partner, Powered Resilience Leader | KPMG in the UK
E: andrew.husband@kpmg.co.uk



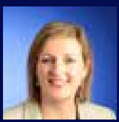
Lulu O'Leary
Partner, Insurance Transformation | KPMG in the UK
E: lulu.oleary@kpmg.co.uk



Ashley Harris
Director, Bank MC Operations | KPMG in the UK
E: ashley.harris@kpmg.co.uk



Nick Todd
Director, Insurance Transformation | KPMG in the UK
E: nicholas.todd@kpmg.co.uk



Becky Wilson
Senior Manager, Insurance Transformation | KPMG in the UK
E: rebecca.wilson1@kpmg.co.uk

kpmg.com/uk

CREATE | CRT136433 | May 2021