KPMG

Getting ahead of the game on Operational Resilience

What should you focus on now?

December 2019

kpmg.com/uk

N
S

Operational Resilience in insurance: Making it part of your DNA

Now that the expected consultation papers have been published by the Prudential Regulation Authority (PRA), Financial Conduct Authority (FCA) and Bank of England (BoE), we have a clearer view as to how the new Operational Resilience regulatory regime is taking shape, and how firms in the wider insurance ecosystem will be affected. Preparing early will reduce costs and disruption down the line.

This brief publication looks at:

— How the regime will affect the insurance sector, and what we can learn from others?

— What could it mean for my firm and where to focus?

— What questions should we be asking?

— What can my firm do to get a head start?

Key question: How can my firm get ahead of the game?

What can we learn from others?

What will Operational Resilience mean for the insurance sector?

The background – why should insurers address Operational Resilience now?

Regulation to date has focused more on financial, rather than Operational Resilience. New regulations will bring more focus onto firms' operational robustness, emphasising the role of the Chief Operations Officer as responsible senior management function for implementing operational resilience policies and reporting to the Board.

Regulators are assuming disruptions will occur. Firms need to have robust operational resilience plans in place, with a clear view on vulnerabilities across their important business services.

Firms can enhance their Operational Resilience immediately by addressing known problem areas and by embedding Operational Resilience practices in their BAU activities.

We have business continuity plans in place – does that mean we will be compliant?

A key challenge for firms is to change their view of business from a functional to an end-to-end service and customer perspective across the value chain, considering the ecosystem as a whole.

For example, today's business continuity plans are typically siloed by function and based on discrete operational KPIs. True Operational Resilience works across end-to-end business services and looks at business outcomes from a customer perspective, embracing third parties involved in the service.

Regulators will be expecting Boards and senior management to be responsible for Operational Resilience oversight and governance.

Clarity of planning and reporting will be an essential component to help them fulfil their responsibilities.

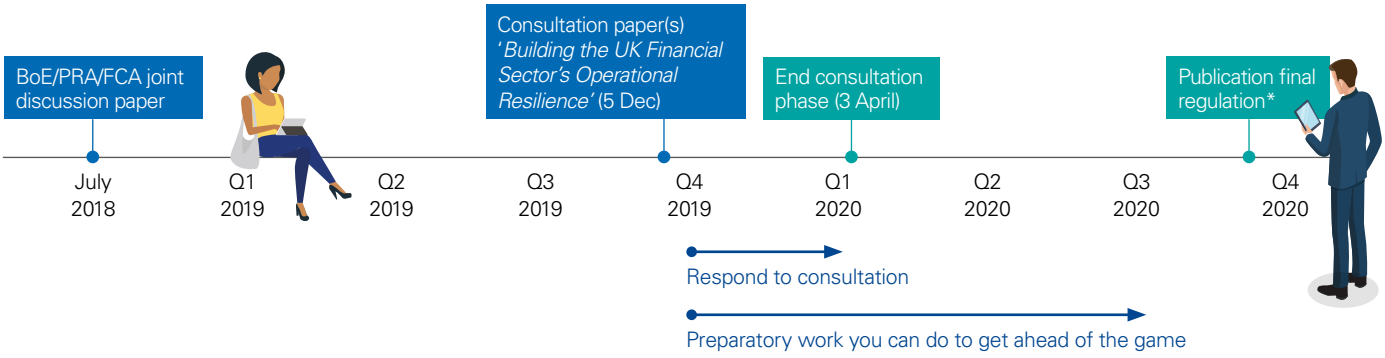
How is the regulation likely to work?

Joint supervision across FCA, PRA and the Bank of England (BoE).

Each firm will need to define disruption scenarios across the different 'pillars' of technology, suppliers, property, information, and people, and will also need to set impact tolerances for important business services. These tolerances define the maximum tolerable duration of disruption and could cover other parameters such as value and volumes that the Board is willing to tolerate. The tolerances you set will be in the form of customer outcomes or metrics and may include customer response times, work backlogs and data integrity as well as other service outages.

The important business services will need to be tested regularly using service resilience assessments.

Timeline



* Please note: No timelines for final regulation have been communicated yet by the regulator. The timeline reflects KPMG's view.

Your impact tolerances will reference a set of perils or disruptors, assuming that one or more perils will occur. For example:

- Physical: natural hazards or sabotage
- Cyber
- IT outage
- Third party failure
- Data security failure

Firms are responsible for their suppliers' resilience.

Expected supervision regime and lines of enquiry

Supervision is expected to be principles-based and the regulators will want to verify that you are taking the appropriate steps to define, implement and embed Operational Resilience sustainably.

It is envisaged that supervision will follow four modes:

1. Sector-wide stress tests*
2. Review how impact tolerances are set and governed
3. Check firms' understanding of how their systems, processes and people will drive resilience
4. Ability of firms to recover from disruption

The BoE will use stress tests to ascertain whether firms meet certain resilience impact tolerances.

* Likely to be used in banking. To be confirmed for insurance.

Our market insights

- Responsibility for driving Operational Resilience across the firm is often unclear, reflected in operational activities that are often not integrated or silo-ed.
- Operating models tend to be functionally designed, and Operational Resilience teams struggle to get buy-in from business and establish a cross-functional view.
- Firms' Operational Resilience often stops at the boundaries of the organisation, but does not consider the entire ecosystem.
- Operational Resilience is not the same as or an extension of operational risk management – just like solvency capital management is not the same as financial control.
- Banks have already started resilience assessments and design initiatives and are ahead of the insurance sector. The regulators will be expecting the insurance sector to engage across the board. In insurance, we have seen more interest so far from brokers.
- Engaging with Operational Resilience now means you may be able to incorporate any requirements into existing transformation programmes. Waiting until later would end up costing you more.
- We think the toughest challenges for firms will be:
  1. Setting the right impact tolerances
  2. Embedding Operational Resilience into the operating model and culture
  3. Updating your resilience regime as likely perils change
  4. Clarity of planning and reporting to the Board
  5. Operationalising resilience tracking through data and tools.

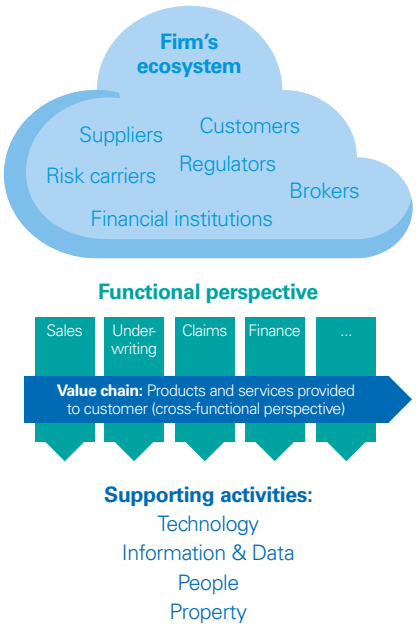
What can we learn from the banking sector

- Big 4 banks are all implementing Operational Resilience but there isn't a standardised approach yet.
- Sponsors vary but typically COO, CRO, Chief Information Security Officer.
- Some newer entrants are thinking about how Operational Resilience can give them a competitive advantage.
- Defining a good service architecture is key. Banks are using pilots and are enhancing existing MI.
- Challenges remain in the transition from design to effective implementation, in scaling up and in cultural embedding.
- Operational Resilience is not a risk and control exercise, but is about customer outcomes. It must be business-driven.
- Impact tolerances are not the same as risk appetite or recovery time objectives – they assume that a disruption will occur and define the extent to which a firm should tolerate disruption.

What could it mean for my firm?

What all firms will need to consider:

Understand how this differs from business continuity and other established risk and governance frameworks	This will require education at a number of levels: Board, executives, senior managers, risk functions.
What will Operational Resilience mean?	Set a vision and strategy for Operational Resilience. Key challenges will be the definition of end-to-end business services and the setting of impact tolerances.
What work do I need to do to implement this?	Once you have a vision, strategy and tolerances, you will need a diagnostic to understand gaps. This could be a good opportunity to go beyond minimum compliance and address any specific weaknesses or issues in your operational value chain.
What is the right governance model for this going forward?	This has to be governed from the Board but you may need to update your operational risk and governance regime to incorporate the 'end-to-end' and 'business outcome' elements of the Operational Resilience regime.
Embedding Operational Resilience into the firm's DNA	Education and vision are really important here, as well as MI and a performance management regime. Insurance firms are traditionally organised by function which may make implementation of an end-to-end resilience regime more challenging.
Focus on the whole ecosystem	Consideration of the firm's ecosystem as a whole is crucial in understanding key resilience risk areas along your end-to-end business services. This will include distribution, operational and financial partners.



Where should my firm be focusing?

These are some examples of the likely key areas of Operational Resilience focus for different insurance players:

Broker

End customer interactions including new business, queries and claims

- Likely to be the primary business outcome of interest to the FCA
- Where you need rapid responses from capacity providers or claims outsourcers, the end-to-end processes between organisations will need to be resilient

Links to software house or insurer quote engines

- Are your insurers' and providers' resilience plans up to scratch?
- What data and processing linkages do you need with your partners to stay within your impact tolerances?

Primary carrier

Customer and broker interactions including new business, queries and claims

- You may have business continuity plans in place
- What needs to be in place in claims and underwriting to ensure end-to-end resilience?
- If you rely on third parties for technology processing or overflow, are they sufficiently resilient to meet your impact tolerances?

Book-bind-issue processing

- Middle office delays or failures may impact business outcomes for the insurer and their customers

Balance sheet funding and hedging

- Inability to perform this activity could give rise to ongoing financial and therefore operational viability issues

Other players

MGAs: new business and claims processing

- Can you rely on capacity providers and claims management partners?

Third parties: Can you use Operational Resilience as a competitive advantage?

- Carriers and brokers will need to factor in your resilience to their end-to-end business outcomes

Re-insurer

Facultative treaties

- If fast response is required to facilitate insurer new business, how can you ensure your firm can operate resiliently?

What questions should we be asking?

Operational Resilience will have an impact throughout your business. Your Board and senior management team will need to address the challenge from a number of angles. Here are some of the questions you may need to ask:

CEO

Operational Resilience is a business imperative – how do I ensure we are tight on this?

How much should we invest in Operational Resilience?

How do I keep my executives accountable for this?

How do we effectively communicate our readiness to the Board and regulators?

COO

How do I write the business case for improving Operational Resilience?

How can I use it as opportunity to strengthen my value chain?

How should the SMF24 accountability work for this regime?

How do I go about ensuring all elements of our ecosystem are operationally resilient?

CFO

We know a shock will hit us – how can I reduce the hit on my bottom line?

What is the right balance between investing in resilience and protecting my P&L?

How do I measure financial return and operational success in Operational Resilience?

Can I reduce my SII operational risk capital requirements?

CRO

How do I make sure the FCA and PRA understand and are convinced by our Operational Resilience plans?

How do I get the Board to agree the right vision and parameters for Operational Resilience?

Operational Resilience is different from business continuity – how do I get that bedded in to our culture?

Chief Customer Officer

How do we use customer feedback to help set impact tolerances?

What's the best way of communicating with customers during disruption?

NED

My Board needs a vision and strategy for this – how can I help the execs to create one?

How do we hold the execs accountable for execution of the Operational Resilience strategy?

How much should we focus on Operational Resilience?

You will have different choices to make to comply with this new regime, including:

— How tight should your impact tolerances be?

— Whether to bring some activities back in house

— Whether to change third party partners to increase end-to-end resilience

— Making data interfaces more robust, particularly between organisations

— Harmonisation and evolution of your technology landscape

Determining which areas to focus on will require a business case. Writing a business case around regulatory change is not always straight forward. This will require strong and informed debate around the Board and Executive Committee tables.

Strong Operational Resilience in its very nature brings significant business advantages

Weaker Operational Resilience

Pros
- Not resource intensive
- Perhaps less internal disruption from resilience improvement projects

Cons
- Less resilient business
  - — New business revenues may reduce
  - — Customers may lose faith
  - — Potentially more costly to recover
- More regulatory scrutiny
- Reactive approach

Stronger Operational Resilience

Pros
- Proactive approach to Operational Resilience should improve operations and business in general as it is a sharpening of the ecosystem
- Opportunity to address supply chain weaknesses or issues
- Customer disruption reduced relative to competitors
- Integrating Operational Resilience into existing transformation programmes should also reduce total investment

Cons
- Resource intensive
- Cultural and organisational change required

How can I get a head start?

KPMG's eight key steps to Operational Resilience implementation

Operational Resilience takes a holistic business service perspective and considers both horizontal and vertical aspects of an organisation.

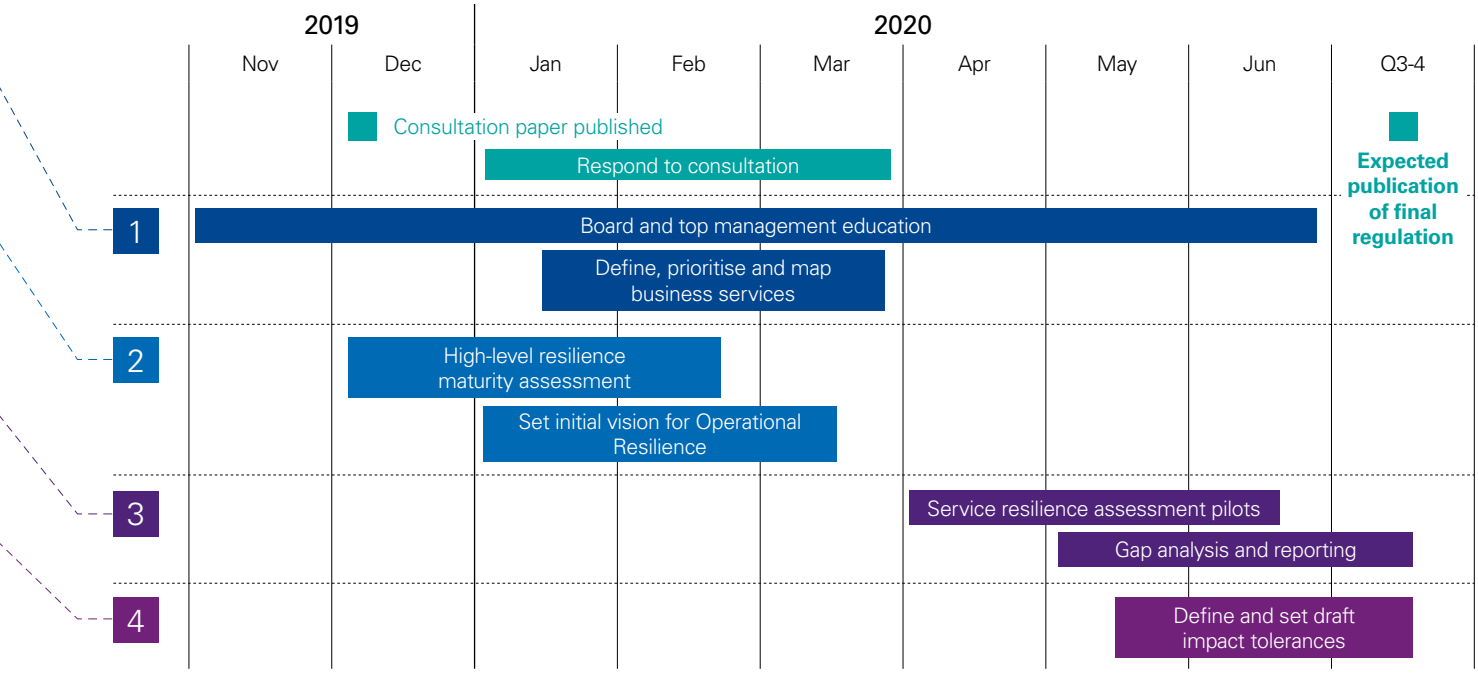
From our expertise in regulatory and operational transformation we have determined eight steps that all firms should follow when complying with this new regime.

Executed carefully, these eight steps will ensure your firm complies with and gets the full benefit of this new Operational Resilience regime.

1	**Define business services architecture**	— Board and top management education — Define and prioritise important business services — Map processes and resources to important business services
2	**Strategy and operating model for Operational Resilience**	— Define vision and strategy — Define governance and ownership for operational responsibility — Implement organisation design and culture
3	**BAU service resilience assessment**	— Assess ability of services to deliver under BAU conditions
4	**Recovery scenario testing**	— Review and define disruption scenarios — Set impact tolerances — Scenario testing against impact tolerances
5	**Emerging threats management**	— Horizon scanning to identify new threats
6	**Reporting, investment and service enhancements**	— Define MI & measurement requirements — Regulatory and Incident information reporting and communications — Build resilience into ongoing or planned operational projects
7	**Recovery planning and management**	— Define and manage appropriate business continuity plans, IT disaster recovery and incidents
8	**Data and tooling**	— Operationalise resilience data and testing on end-to-end basis

How to use the next 6-9 months to prepare

Final regulation publication is not due until Q3 2020, but your firm could use this period to prepare. This should reduce the overall cost of any implementation, and will help ensure any intervening transformation programmes are aligned your firm's resilience regime. Here is an example pilot programme.



Some major players are already getting ahead:

UK retail insurer

Challenge: Client asked KPMG to perform an Operational Resilience assessment of FNOL activities.

Scope: Define impact tolerances, enhanced data mapping of business service, resilience assessment, definition of resilience MI & metrics and scenario testing.

Approach: Review client's existing resilience regime against five resilience pillars: cyber, IT, property, people and suppliers. Identify upgrades required for new regulatory regime. Desktop scenario testing.

Outcomes: Client has good overview of how activities connect across different services, resilience frameworks defined, gaps identified in FNOL and implementation approach defined for other business services.

UK universal bank

Challenge: Bank asked KPMG to assess current Operational Resilience approach against principles in 2018 Q3 discussion paper.

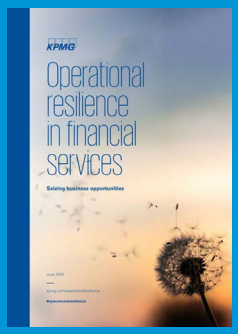
Scope: Discussion paper response, business services definition, gap analysis, creation of full Operational Resilience framework, mobilisation of implementation programme.

Approach: Mapping of value streams and economic functions to business services, definition of what good looks like for resilience, development of Operational Resilience strategies.

Outcomes: Good client understanding of new regime, MI approach and dashboards, templates developed, ongoing guidance and support.

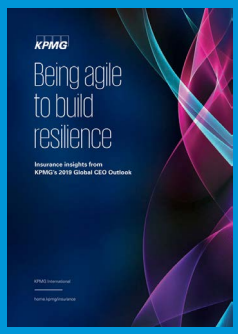
Other publications

Operational resilience in financial services
Seizing business opportunities – June 2019



Click here

Agile or irrelevant
Redefining resilience – 2019 global CEO outlook



Click here

10 conversations about operational resilience

Click here

Contacts

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

David Miller
Partner, Insurance Risk & Regulatory
KPMG in the UK
E: david.miller@kpmg.co.uk

Andrew Husband
Partner, Head of Operational Resilience and Banking Lead
KPMG in the UK
E: andrew.husband@kpmg.co.uk

Jon Dowie
Partner, Technology Risk
KPMG in the UK
E: jon.dowie@kpmg.co.uk

Thomas Rauschen
Principal, Insurance Operations
KPMG in the UK
E: thomas.rauschen@kpmg.co.uk

Matthew Martindale
Partner, FS Cyber
KPMG in the UK
E: matthew.martindale@kpmg.co.uk

Douglas Dick
Director, Technology Risk
KPMG in the UK
E: douglas.dick@kpmg.co.uk

Matthew Francis
Director, Insurance Regulation
KPMG in the UK
E: matthew.francis@kpmg.co.uk

kpmg.com/uk