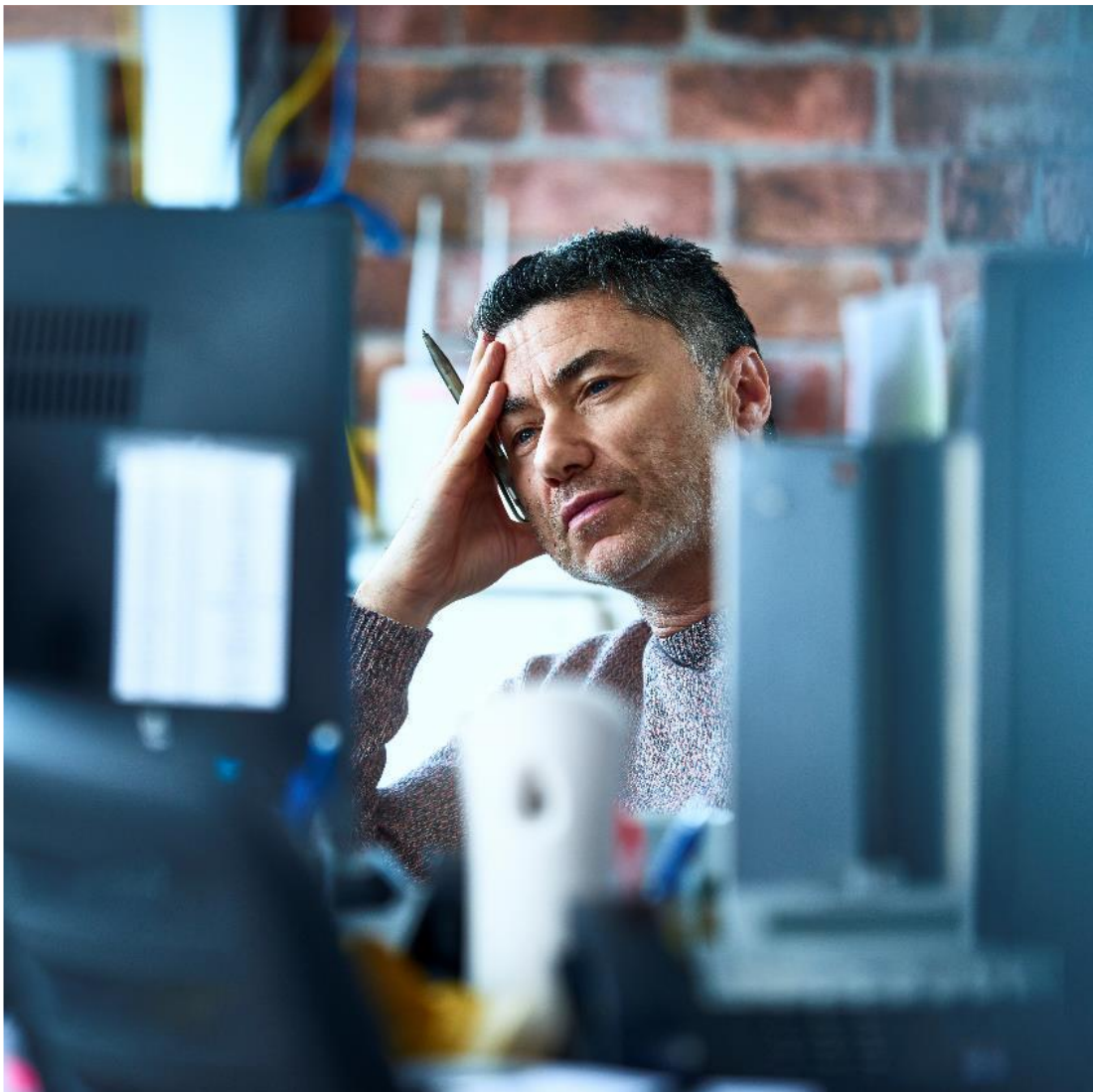
Operational resilience: How to set and test impact tolerances

February 2020



pwc

Contents

Foreword

This is a revised version of a white paper, originally published in October 2019, to reflect the consultation papers issued by the UK supervisory authorities on 5 December 2019 as well as our experience in working with clients on this subject. While the overall methodology remains the same, the update now includes excerpts of the consultation papers to increase firms' understanding of key concepts.

Until the point at which final policy statements are published by the supervisory authorities, the definitions and guidance remains draft. The content of this white paper will therefore evolve further in 2020.

Click here to access a summary of the main points from the consultation papers.

Introduction to operational resilience

With the 2018 publication of a joint discussion paper[1] (DP) on operational resilience by the Bank of England, Prudential Regulation Authority and the Financial Conduct Authority (together the 'supervisory authorities'), the topic of operational resilience was pushed firmly toward the top of the agenda for boards and senior management of financial institutions and financial market infrastructures, FMIs, (hereafter referred to as 'firms'). The DP set out a structure for improving the operational resilience of all firms in the financial services sector, and was the first document by national competent authorities to put forward ideas on delivering a holistic approach to operational resilience.

UK supervisory authorities' definition of operational resilience: the ability of firms and FMIs and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions.

Since then many firms have started to shift their thinking in line with the principles in the DP, even though this has not yet been translated into final rules. In many cases, this is because supervisory authorities have been calling upon them to do so; however, firms also recognise the commercial imperative for action. In December 2019 the supervisory authorities published a suite of consultation papers including draft policy and supervisory statements aligned to their respective objectives[2].

Firms are expected to improve their operational resilience through:

i. Prioritising the things that matter (identify important business services and map their delivery)

ii. Setting clear standards for operational resilience (referred to as impact tolerances)

iii. Investing to build resilience (so they can remain within impact tolerances).

The proposed transition arrangements indicate that firms 'must be able to remain within their impact tolerances as soon as reasonably practical, but no later than three years after the rules come into effect'[3]. If the final policy is published by the end of 2020, with a 12 month implementation period, this would mean the end of 2024 at the latest. The time to act is now.

Proposed scope of the new policy guidelines

Whereas the 2018 discussion paper suggested that all financial services firms could be in scope, the FCA CP[4] suggests a narrower scope of firms made up of:

- c. 1,050 banks, building societies, PRA designated investment firms, Solvency II firms, Recognised Investment Exchanges, Enhanced scope SM&CR firms and third-country branches
- c. 1,100 Payments Institutions, Register Account Information Service Providers and Electronic Money Institutions.

In addition the policy changes would apply to the FMIs supervised by the Bank of England. Firms not in scope may choose to adopt the guidelines on a voluntary basis; but at the very least they are expected to meet their existing operational resilience obligations.

It is clear that impact tolerances are the centrepiece of the supervisory authorities' framework on operational resilience. Our work over the last 7 years has helped clients and regulators to shape their views on this topic. This PwC white paper provides a structured way of defining and testing them.

It should be remembered that the supervisory authorities may well change aspects of their proposals following the consultation period, so the content of this white paper may evolve further in line with fresh guidance.

---

[1] 'Building the UK financial sector's operational resilience' (PRA DP01/18; FCA DP18/4)

[2] For a summary please read: 'PwC Hot topic: UK supervisory authorities reveal more on how firms should build their operational resilience'

[3] FCA paper CP19/32, section 5.23

[4] FCA paper CP19/32, Annex 2 – Cost Benefit Analysis, point 27

Introduction to impact tolerances

Impact tolerance: The maximum tolerable level of disruption to an important business service, including the maximum tolerable duration of a disruption[5].

The consultation papers reveal much more detail on the regulators' views of impact tolerances:

- Setting impact tolerances is a tool for planning and discovery purposes.
- Firms should set them at least annually for their important business services and important *group* business services.
- Firms should identify specific metrics for the maximum tolerable level of disruption. These should be measures that identify: harm to consumers or market participants; harm to market integrity; threat to policyholder protection; threat to safety and soundness; or threat to financial stability.
- An impact tolerance should relate to a single disruption as the concept is designed to identify how quickly a firm should be able to restore delivery of service after disruption. In the context of setting impact tolerances, firms are not expected to consider the cumulative impact of multiple incidents over, say, a 12 month period. However, this is relevant in the context of good risk management.
- Dual-regulated firms will be expected to set and manage up to two impact tolerances for each of their important business services: one at the first point at which there is an intolerable level of harm to consumers or market integrity (FCA); and another at the first point at which financial stability, a firm's safety and soundness, or policyholder protection is put at risk (BoE/PRA).
- In such instances regulators recognise that it may be appropriate for firms to focus on the impact tolerance which has the shortest duration when prioritising actions; but the 'other' regulator will expect to see that scenarios have been considered that may test the longer tolerance even if the mitigants are similar.
- Firms should not set their tolerances at excessively high levels, which is likely to suggest that they are able to manage service continuity within them for all scenarios without any investment.

In addition, the draft policy and supervisory statements include factors which firms should consider when setting impact tolerances with significant crossover into those to determine which business services are important[6].

Such additional detail will undoubtedly help firms to start working on their impact tolerances, but the exercise will still prove to be challenging, especially for dual-regulated firms which need to understand the hierarchy of potential tolerances which could be set, and managing against multiple reference points.

Annex 1 includes a comparison of impact tolerance and risk appetite.

[5] Building operational resilience: impact tolerances for important business services ('Joint CP cover paper'), section 3.5

[6] FCA CP19/32, Appendix 1 Draft Handbook Text, 15A.2.7 and PRA CP29/19 Appendix 3 Draft Supervisory Statement, 2.5

Our approach to setting impact tolerances and testing them

Through the experience we have gained in working with clients on this topic, and in discussions with regulators, we have formulated a five stage approach for firms to set their impact tolerances and test their ability to remain within them. The first stage, 'identify and map services', is considered a prerequisite for firms looking to set impact tolerances. This white paper describes what is involved in each stage.

Develop self-assessment document

1 Identify and map services (pre-requisite)	2 Gather baseline data	3 Set impact tolerances	4 Scenario test	5 Ongoing governance
Determine which business services are 'important' and map the resources to support delivery.	Gather data to show the day-to-day functioning of the business service.	Assess *how* a disruption may impact end users of the business service and propose impact tolerances.	Test the firm's ability to manage service delivery within impact tolerances in different scenarios.	Develop a testing programme and monitoring regime for ongoing assurance. Sign off self-assessment.

We have developed a bridge analogy to illustrate how these five stages can be delivered.

Introduction to the bridge analogy

Consider a firm that owns a one-way bridge across a river to enable people to drive from one side to the other. The firm identifies an important **business service** it provides as: **crossing the river**.

Each vehicle crossing the bridge represents a **transaction,** and drivers pay a fee (a toll) to do so.

The total **capacity** of the business service is limited to four lanes and is represented by how many vehicles can cross at any given time. **Disruption** to the bridge may force the firm to close one or more lanes, impacting the ability of vehicles to cross and limiting the capacity of the service.

The firm can **communicate** with customers in various ways including smart motorway signs and local media.

We will also assume a parallel to the financial services regime and assume that the **firm is regulated by two authorities**: one focused on the potential harm to consumers; and the other focused on the firm's financial viability and the stability of the market.

We will apply this analogy to the five stages to show how this firm could define its impact tolerance.

Stage 1 – Identify and map services

A prerequisite to starting work on impact tolerances is to identify, at a firm level[7], at least one important business service. A methodical way to approach this would be to identify the full universe of business services a firm delivers to its customers and use a set of criteria to shortlist those which are 'important'. At this point firms will need to consider the risks that disruption to each business service pose to the supervisory authorities' objectives. This analysis will help in considering relevant data points in Stage 2 and tolerance metrics in Stage 3.

> **Important business service**: Means a service provided by a firm or FMI to an external end user or participant where a disruption to the provision of the service could cause intolerable harm to consumers or market participants; harm market integrity; threaten policyholder protection; safety and soundness; or financial stability[8].

The key element here is that it is provided to an **external** end user or participant. Business services, as defined by the supervisory authorities, do not relate to internal functions (e.g. IT department) or processes (e.g. staff payroll). Business services need to be articulated at a level of granularity which enables an impact tolerance to be applied and which supports management bodies in making prioritisation and investment decisions. The CP suggests that firms will be required to identify important business services at least annually, and after a material change to the business. Examples of business services include: ability to check a balance online, provide currency hedging services, administration of investments, or the provision of correspondent banking services to indirect participants.

The firm then needs to understand how each business service is delivered, by mapping the key process steps and defining which resources enable it to be delivered. The service maps must be at a level of detail that helps to identify the resources that contribute to the delivery of each stage, and their criticality.

> **Mapping**: A firm or FMI must identify and document the necessary people, processes, technology, facilities and information (referred to as resources) required to deliver each of its important business services[9].

Firms should identify where these resources are being provided via a third party, whether intra-group or external.

How this applies to the bridge analogy

Moving back to our bridge analogy, the firm identifies an important business service as '**crossing the river**'. The bridge is a key piece of infrastructure for the region with no real alternatives offering a comparable service[10]. The firm breaks it down into five basic process steps.

It can then identify the resources that enable the firm to deliver the service and monitor performance, and impact, as follows:

- Technology: Traffic flow sensors, CCTV, card payment facility, number plate recognition
- People: Maintenance crew, toll collectors, traffic flow controllers
- Facilities: Road bridge, toll booths, remote control centre
- Information: Number plate registration, payment card details
- Third parties: POS payment provider, maintenance contractor firm, driver and vehicle licensing agency.

[7] A later section in this report will cover the concept of important business services at a group level.

[8] Joint CP cover paper, section 2.5

[9] Joint CP cover paper, section 4.17

[10] Assumption: there is a one-way bridge going the opposite way further up the coast which is operated by a different firm.

Stage 2 – Gather baseline data

Once the business service has been selected and mapped out, the firm needs to establish what constitutes business as usual functioning of the important business service. This involves considering possible metrics that can describe the typical functioning of the business service through measuring both outcomes and the resources to deliver the service (i.e. inputs). Agreeing the shortlist of appropriate metrics at this stage is key as they will form the basis on which impact tolerances will be set.

The firm gathers historic data for a given day plus the range of data over an illustrative period (e.g. 12 month high and low), which helps to validate that the impact tolerances, when defined, can still be met during demand peaks or troughs. It is also good risk management practice for firms to undertake wider analysis over an extended period on historic failures, such as the number of outages per year and the resulting impact. This will help the firm to validate whether or not the business service is currently working well.

How this applies to the bridge analogy

The firm identifies a series of different metrics which can describe the functioning of the business service:

Measures of direct impact of operational disruption

1. Total number of vehicle crossings completed[11].
    a. Of which, number of emergency services vehicles completed.
    b. Of which, number of trade vehicle crossings.
2. Average time to complete a crossing (including queueing at the toll point).
3. Average wait time to pay at toll point.
4. Total revenue collected at toll point.

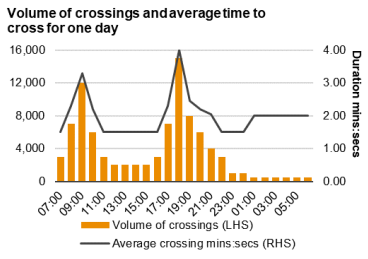
Measures of indirect impact of operational disruption

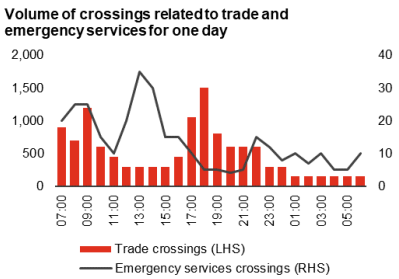
5. Loss data from fraudulent transactions.
6. Regulatory fines or contractual penalties applied as a result of breaches (e.g. on availability of service).
7. Social media sentiment (positive and negative).
8. Newspaper coverage (column inches).

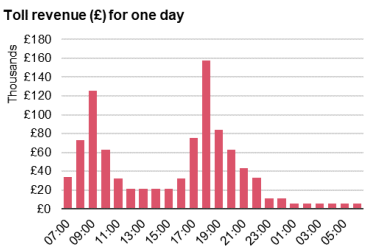
Key risk indicators to help predict future operational disruption

9. Historic incident trend data including root cause analysis.
10. Average speed of vehicles crossing the bridge.
11. Volume of payments by type: cash, debit card, and credit card.
12. Average payment processing time (and variability) by type.

The firm shortlists key metrics as 1 (including a and b), 2 and 4 with example data shown below.







[11] It is important to consider the types of vehicles which use the bridge to cross the river as disruption is likely to have a more significant impact on certain users, for example where lives are put at risk (1a), or where commercial supply chains may be affected (1b)

Stage 3 – Set impact tolerances

Armed with the shortlisted metrics and baseline data (from Stage 2), and the understanding of how end users are impacted in the case of disruption (from Stage 1), firms can then start defining their standards of resilience. This ultimately entails quantifying how a disruption to an important business service could impact different customer groups, the firm, and the wider financial system. Here, firms are looking at the effects without factoring in management actions which would reduce the inherent exposure.

> Metrics could measure the extent of disruption, for example by including the maximum value of disruption, number of transactions or the number of customers affected. All impact tolerances should include the maximum tolerable duration of such disruption, taking into account the criticality of the important business service. However, a metric based on time alone may be insufficient.[12]

Firms should ask themselves at what point disruption would pose a risk to financial stability, safety and soundness, policyholder protection, harm to consumers or harm to market integrity. This will enable the firm to propose tolerance thresholds as a unit of time. Using the duration of any disruption then forms an approximate measure of impact, and this has the advantages of being easy to track and ensuring consistency across firms.

> A firm regulated by both the PRA and the FCA could have up to two impact tolerances for each important business service – one considering financial stability, safety and soundness and policyholder protection, the other set with reference to consumer harm and harm to market integrity. […] The two impact tolerances may be the same for each or they may differ[13].

The proposed guidance will result in solo-regulated firms having one impact tolerance per important business service, and dual-regulated firms having two.

How this applies to the bridge analogy

Disruption to the bridge could have a range of consequences which can be grouped together such as[14]:

- Citizens are unable to complete journeys[15]
- Vulnerable lives are put at risk where emergency services are impeded.
- The flow of goods is disrupted and services are not completed.
- The firm's profitability is hit by lost revenue and additional costs through restorative repairs, penalties and fines on a low-margin business service.
- The firm's cashflow is jeopardised as toll receipts are interrupted.
- The firm's reputation is damaged, impairing its ability to win future contracts.
- The region's reputation is damaged, impairing its ability to attract investment in businesses and trade, which has wider socio-economic implications (e.g. job growth).

Harm to consumers

Risks to firm safety and soundness

Risks to financial stability

Having considered the potential impacts the firm identifies that first to materialise in a disruption would be harm to consumers. A prolonged period of disruption could have significant financial implications for the firm putting its safety and soundness at risk.

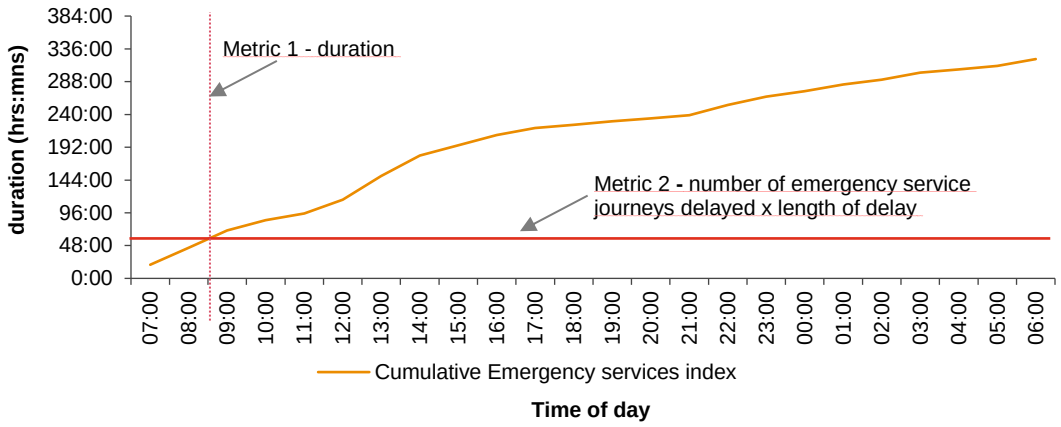
To define impact tolerance limits, the firm assumes that the business service is unavailable and estimates the maximum tolerable level against the key metrics: 1) number of hours of delays to emergency services vehicles; and 2) loss of revenue during the disruption.

[12] Joint CP cover paper, section 3.3
[13] Joint CP cover paper, section 3.8-3.9
[14] Harm to market integrity and policyholder protection are not considered as relevant to this particular business service
[15] Citizens will use the bridge for a variety of reasons and therefore disruption will have differing degrees of impact from inconvenience to harm

Regulator A: Harm to vulnerable consumers

'Delay to journeys' is a tangible impact with potentially severe consequences. Emergency services are forced to find alternative methods of crossing, adding one hour to journey times. The threshold is determined at a point where the risk of loss of life is deemed to have increased substantially based on analysis of available data.

Cumulative emergency service impact for one day (journeys delay time)

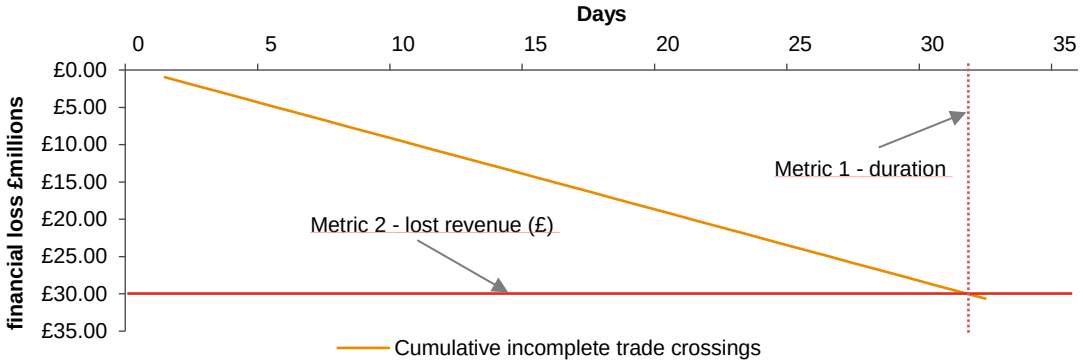


The resulting impact tolerance = 2 hours of total disruption (i.e. zero capacity) **and** >50 hours of delayed emergency services journeys.

Regulator B: Safety and soundness of firm

Financial loss is captured through lost revenue levied as a result of contractual or regulatory breaches. The threshold is determined at a point where the financial loss will have a detrimental impact on the firm's viability. For this first round of setting tolerances the firm has excluded assumptions on penalties (e.g. regulatory fines). However, analysis of previous fines for similar events could be used to further calibrate the tolerance in the future.

Cumulative financial loss (£m) vs. forecast day-by-day



The resulting impact tolerance = 32 days of total disruption (i.e. zero capacity) **and** >£30m reduction in revenue.

Stage 4 – Scenario test

Scenario testing: is the testing of a firm or FMI's ability to remain within its impact tolerance for each of its important business services in the event of a severe (or in the case of FMIs, extreme) but plausible disruption of its operations. In carrying out the scenario testing, a firm must identify an appropriate range of adverse circumstances of varying nature, severity and duration relevant to its business and risk profile, and consider the risks to delivery of the firm or FMI's important business services in those circumstances[16].

Firms need to conduct scenario testing using severe but plausible scenarios to assess their ability to remain within their defined impact tolerances. Tests should include failures within their control (e.g. IT system failures) as well as those outside of their control (e.g. cyber attack or disruption to power supply).

The supervisory authorities guide firms to consider a number of different elements when developing a testing plan[17]:

- The type of scenario testing. For example, whether it is paper-based, simulations or live-systems.
- The frequency of the scenario testing - firms that implement changes to their operations more frequently should undergo more frequent scenario testing.
- The scenarios for which the firm expects to be able to remain within its impact tolerances and those for which it does not.
- The number of important business services tested - firms that have identified more important business services should undertake more scenario testing to reflect this.
- Testing the availability and integrity of resources. A business service that is available but has compromised integrity is not remaining within the impact tolerance. For example, if a firm resumed service to remain within an impact tolerance when the firm knew there was a significant risk of spreading a computer virus.
- How communication strategies can be used to act quickly and effectively to reduce disruption by providing clear, timely and relevant information.
- How the firm's environment is changing and whether this will give rise to different vulnerabilities.

During the exercise, firms will need to make assumptions in determining the effectiveness of actions, based on, for example, whether contingency measures have been used before and what outcome they generated. This is important for a fair test of the expected response. Firms should consider the full operating landscape here, including any assumptions on dependencies with suppliers or what peers are doing.

During the exercise, firms should prepare documentation showing the steps they went through and capture lessons-learned afterwards. The results can be used to validate the proposed impact tolerances and to agree remedial actions, where appropriate including proposed investment cases. Critical to this stage is bringing together the right team of people to conduct the exercise, particularly those with individual responsibility for areas which are impacted, as well as those responsible for the resources that provide contingency or recovery measures.

[16] Joint CP cover paper, section 4.14

[17] The PRA and FCA include subtly different requirements so this list is a combination of the two: FCA paper section 6.16 and PRA paper section 4.19

How this applies to the bridge analogy

Scenario: On Monday 20 May 2019 at 07:00 two lorries collide and cause a pile-up with three other cars. The wreckage spans all lanes of the bridge with no way for other vehicles to get through. One of the lorries partially ruptures the wall on one side of the bridge. An unidentified liquid chemical has started leaking from the cargo of one of the lorries. Several of the passengers are trapped in their vehicles. At this point it is not known how serious the injuries are.

Assumptions made by the firm:

- The incident was identified by the control centre via remote cameras on the bridge
- There have been no explosions or fires
- There is a weather warning for high winds.

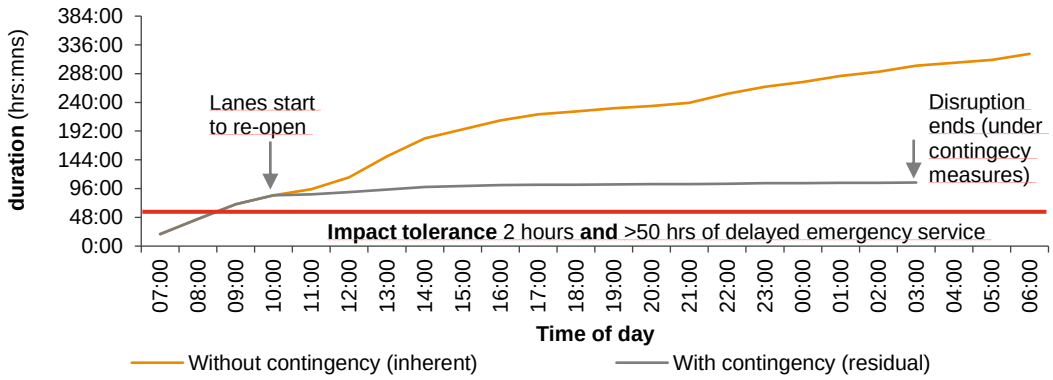
We now see what actions the firm could take and the expected effects of the actions in managing the incident. Actions could include, but are not limited to:

1. Contacting emergency services to alert them of the incident
2. Closing the toll gates remotely to prevent further vehicles from entering the bridge
3. Alerting local media to discourage further travel via this route
4. Dispatching engineers to assess structural damage to the bridge
5. Arranging for lifting equipment (e.g. crane) to remove wreckage
6. Arranging alternative crossing routes to support customers (e.g. chartering a ferry)
7. Identifying customers who are trapped on the bridge, especially those that are vulnerable
8. Seeking to reopen individual lanes at the first opportunity.

Regulator A: Harm to consumers

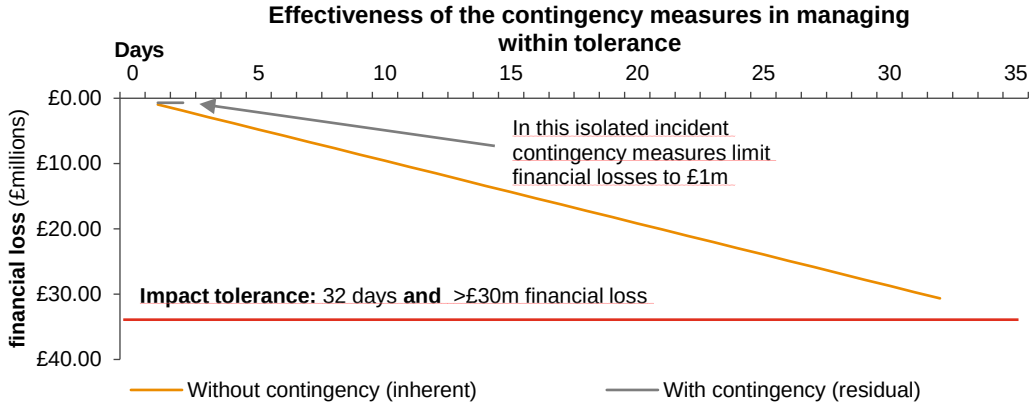
The initial impact is not easily mitigated as vehicles cannot cross the bridge until the wreckage has been partially cleared. Contingency measures therefore take several hours to become effective, reducing the overall impact significantly but still breaching the tolerance threshold.

Effectiveness of the contingency measures in managing within tolerance



Regulator B: Safety and soundness of firm

As a result of the disruption, the firm does not collect vital toll receipts which sustain cashflow and help to manage outgoing costs for third party contracts. Costs for chartering a ferry initially increase the financial impact but as lanes start to open the overall impact is managed within tolerance.



Conclusion: based on this scenario the business service is not considered resilient enough to remain within the proposed impact tolerance for harm, though the firm expects to manage the incident without risks to safety and soundness.

The firm holds a lessons learned evaluation to consider learning points and agree actions, including assessing investment opportunities.

Note, the firm is expected to use variations to the scenario to consider different levels of stress. These could include: number of vehicles included in the collision or the assumed time to determine the nature of the spillage and the risks of intervening prior to this knowledge.

Stage 5 – Ongoing governance

Once the impact tolerances have been defined and tested they need to be agreed by senior management and the board. To do this firms will need to show the relationship between the impact tolerance statements and the board's overarching risk appetite. They must also agree how the board will gain ongoing assurance that the firm can operate within these thresholds through, for example, future scenario testing, management information (MI), and independent assurance. MI should incorporate lead indicators to help monitor changes in the probability of disruption as well as the potential size of it.

The firm will need to ensure that the existing governance framework, including individual responsibilities and committee structures, reflects changes in responsibility with respect to operational resilience. Our work with firms has emphasised how the introduction of a SMF24 (Chief of Operations) role, and the Senior Manager and Certification Regime more generally, has helped to crystallise focus on this topic and move operational resilience from the second to the first line of defence. In addition, SMF6 role holders (Head of Key Business Area Function) should be responsible for embedding operational resilience into their business areas, with individuals taking responsibility for each end-to-end process.

The consultation papers introduce the idea of a self-assessment document, to be made available to regulators on request, which summarises the resilience of a firm's important business services. The box below sets out in more detail the expectations of what this covers.

The self-assessment document should include:

- The firm's important business services.
- The impact tolerances set for these important business services.
- The firm's approach to mapping, including how the firm has identified its resources, and how it has used mapping to identify vulnerabilities and support scenario testing.
- The firm's strategy for testing its ability to deliver important business services within impact tolerances through severe but plausible scenarios, including a description of the scenarios used, the types of testing undertaken and the scenarios under which firms could not remain within their impact tolerances.
- An identification of the vulnerabilities that threaten the firm's ability to deliver its important business services within impact tolerances, including the actions taken or planned, and justifications for their completion time.
- The firm's lessons learned exercises.
- The methodologies used to undertake the above activities.[18]

[18] FCA paper CP19/32, section 7.16. Note, this guidance differs somewhat in the other CPs.

How this applies to the bridge analogy

Having completed the first cycle for an important business service, setting and testing the impact tolerances, the board signs off the resulting documentation and agrees updates to the firm's governance framework to ensure clear individual and collective accountabilities. This would include discussion and agreement of:

- Self-assessment document to share with regulators (on request)
- Updates to existing risk MI reports
- Terms of reference for key committees.

The firm prepares a summary of the operational resilience of each important business service for use in the self-assessment document and reporting to key resilience committees. This would include reference to scenario testing undertaken, an assessment of the resilience of underlying resources, and remediation activities to improve resilience of the business service.

Business Service: Crossing the river

Impact tolerances

Harm to consumers
- 2 hours of total disruption **and** >50 hours of delayed emergency services journeys.

Risk to firm's safety and soundness
- 32 days of total disruption **and** >£30m of lost revenue.

Scenario testing

E.g.
1. Multiple vehicle collision.
2. Protestors blockage bridge.
3. Bridge explosion.

Resources: current resilience rating

Key major improvements req'd | minor improvements req'd | no further improvements req'd

Summary of resilience of each resource which supports the business service. Score driven by aggregate view of testing programmes and scale of identified remediation..

People	Processes	Technology	Facilities	Information

Recent incidents

E.g.

Date	Event	Duration[1] (hrs:mins)	Harm (hrs:mins)	Financial impact (£)
1-Jan-20	Vehicle broken down	0:30	0:30	£0
20-Dec-19	Road flooding	3:20	9:15	£31k

[1]Duration of incident where at least 1 lane closed

Key risk indicators (predictive)

E.g.	Current month	12-month average
Volume of traffic vs forecast	+1.2%	+2.3%
Average speed of vehicles	66mph	65.5mph
Red weather warnings forecast: month ahead	0	N/A

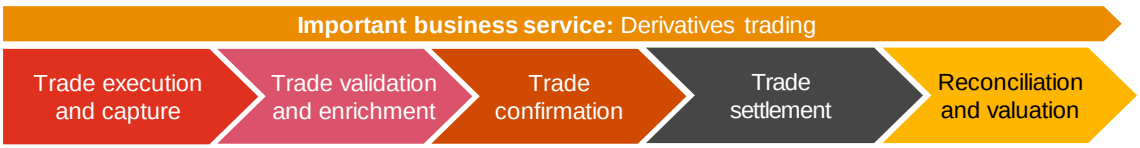
Remediation activities

E.g.
- Replan of 2020-2021 investment budget to address identified vulnerabilities from scenario 1 (due by 30-Apr-2020).
- Start discussions with Fast Ferries Ltd (external third party) to explore chartering vessels for use during severe disruption (due by 30-June-2020).

Relating this back to financial services

Given that the topic of impact tolerances is being introduced with respect to financial services regulation, we need to move away from our analogy and back to reality. In this section, we give some ideas of what impact tolerances could mean for an example business service in each of the three sectors of banking and capital markets, insurance, and asset and wealth management. These have been developed as part of our discussions with firms in these sectors and should be considered as indicative. Firms should recognise the value in the work to reach the impact tolerances and not assume they should be purchased off-the-shelf.

Banking and capital markets example (Firm regulated by PRA and FCA)



Resource examples:

- Technology: Risk management systems; pricing and booking systems; market data repositories
- People: Sales and trading; risk management and finance; operations and technology support
- Premises: Trading floors; back-up premises
- Third parties: External data providers; affirmation platforms; central counterparties
- Information: Trade booking data incl. LEI, reference rates (pricing), FX rates and nostro account data.

Impact tolerance thresholds should be built on duration and could consider other metrics such as:

- Harm to market integrity – the nature of derivatives trading suggests harm to market integrity may be a greater concern than harm to individual market participants who could transact elsewhere. The firm could monitor the number of failed transactions and number of impacted clients over the period
- Financial stability – stability impacts and harm to market integrity are closely linked as harm would manifest more clearly where there is insufficient capacity to trade in the market and therefore risks remain unhedged. The firm could look at stability using the same metrics as for harm (i.e. drop in volume over time) and monitor wider market movements.

Insurance example (Firm regulated by PRA and FCA)

Resource examples:

- Technology: Policy administration system; customer service system; payments infrastructure
- People: Customer service; operations and technology support; treasury, finance and actuarial
- Premises: Processing centre; both onshore and offshore locations possible
- Third parties: Policy administration; data management; risk management; payment issuer
- Information: Policy admin data; inflation rate; asset value; customer vulnerability flags.

Impact tolerance thresholds should be built on duration and could consider other metrics such as:

- Harm to consumers – combination of length of delay to payments and number of payments delayed
- Threat to policyholder protection – use the same metric as for harm to reflect PRA objective on acceptable degree of continuity for policyholders' cover for the return of premiums paid.

Asset and wealth management example (Asset manager regulated by FCA only)

Resource examples:

- Technology: CRM system, order management system, trading system
- People: Client service team, portfolio management, Middle office
- Premises: Client service centre, front office location, middle office location
- Third parties: Custodian, fund administrator
- Information: Customer details, order details (share class, units ordered, price, time).

Impact tolerance thresholds should be built on duration and could consider other metrics such as:

- Harm to consumers – a combination of £ value of outstanding orders multiplied by the length of delay.

Group business services

In its consultation paper the PRA proposes that a firm's self-assessment should cover the group[19], where applicable. This would require firms to identify a 'proportionate number' of important group business services and respective impact tolerances for those parts of the group other than the firm, which are not subject to individual requirements, yet can materially affect the group or UK financial system.

> **Important group business service** means a service provided by a member of a group (other than the firm) to an external group end user which, if disrupted, could pose a risk to: (1) the stability of the UK financial system; (2) the firm's safety and soundness; or, in the case of insurers, (3) an appropriate degree of protection for those who are or may become the firm's policyholders.

This can be brought to life with the following example:

- A group with UK headquarters has a business unit operating in Asia, serving regional clients and operationally independent of the UK business. If a disruption of that business unit could pose a risk to the stability of the UK financial system, the safety and soundness of the UK firm or an appropriate degree of protection for insurance policyholders, it would be prudent for the group's board to satisfy itself of the business unit's operational resilience.

This PRA proposal would require firms to cast their analysis wider than the original thinking in the discussion paper.

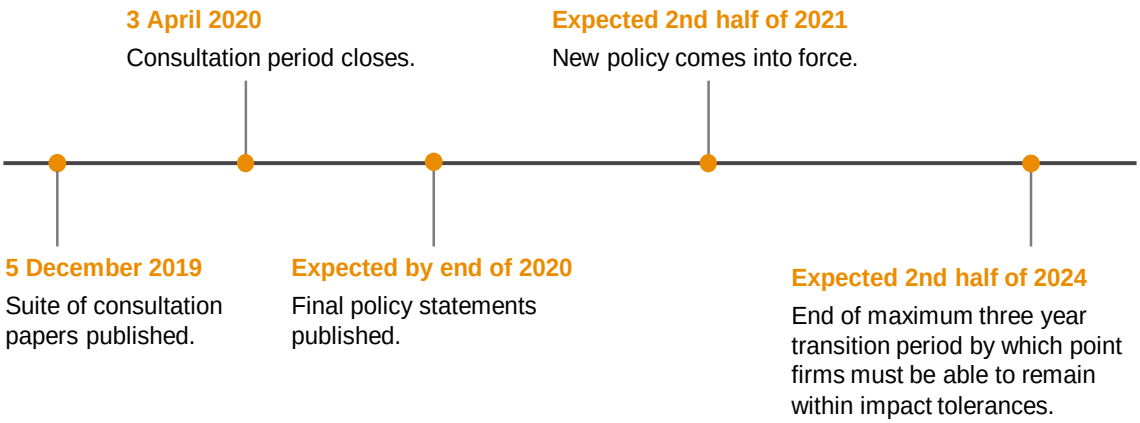
[19] PRA paper CP29/19: section 5 Groups

Regulatory timeline – next steps

The timeline below sets out next steps from the consultation paper. It is important to remember that the policy changes remain in draft until final publication. It is possible that there will be changes through the consultation period.

Firms can expect a transition period post the introduction of the new policy, but the expectation is that action is taken 'as soon as reasonably practicable' and is subject to regulatory discretion.

Alongside the consultation, the supervisory authorities will respond to the Treasury Select Committee on its final report into IT failures in financial services (summary link). In addition, the FCA will confirm its approach to EBA guidelines on ICT (information and communication technology) guidelines and further clarify the links with the operational resilience policy.



Outside of the UK, we have also seen a consultation on operational resilience by the European Commission[20] and expect to see a publication from the Basel Committee on Banking Supervision in 2020.

Final thoughts

Impact tolerances will form a critical element of the regulatory approach to operational resilience. They provide firms with a yard stick to measure current resilience, and regulators with the opportunity to compare firms and consider the aggregate for the wider ecosystem. There is a danger, though, that firms become so engrossed in the science to analyse data and determine tolerance thresholds that they lose sight of the overarching aim. **This is all about building resilience to ensure the continuity of firms' most important business services.** Senior management must ensure there is clear accountability for driving this work, and that the board has sufficient knowledge and skills to enable them to provide robust challenge and oversight. As the PRA states: 'board leadership is necessary, in part because strategic decisions about budgets and spending has implications for a firm's operational resilience'[21].

The 'gold standard' here would be for firms to be able to continue operating their services throughout any severe but plausible operational incidents through effective response strategies. The use of concepts like impact tolerances are a means to end; to help prioritise where investment is best spent to increase resilience. Firms should not be afraid to take the first step on the journey to greater operational resilience.

[20] EC: Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure

[21] PRA paper CP29/19, section 1.12

Annex 1: A comparison of impact tolerances and risk appetite

The supervisory authorities have not changed their view that impact tolerances are different from risk appetite. Unlike a risk appetite, impact tolerances assume a particular risk has crystallised. A risk appetite is the amount of risk that a firm or FMI is willing to take in pursuit of its strategic objectives.

Risk appetites focus management attention on managing the likelihood of operational risks occurring, and the impact if they do. The introduction of impact tolerances will increase the focus of firms and FMIs on their operational resilience before operational risks have crystallised. This should increase their capability to survive severe (or in the case of FMIs, extreme) disruptions when risk appetites are likely to have been exceeded. Impact tolerances are also set only in relation to harm to consumers or market participants, harm to market integrity, or threats to policyholder protection, safety and soundness, and the wider financial sector.[22]

We have clarified this further in the table below:

	Risk appetite[23]	Impact tolerance
Starting point	Firm objectives	Supervisory authority objectives
Relates to	Material risk types	Important business services
Definition	The aggregate level and types of risk a financial institution is willing to assume within its risk capacity to achieve its strategic objectives and business plan.[24]	The maximum tolerable level of disruption to an important business service, including the maximum tolerable duration of a disruption.
Quantification and limits	Includes quantitative measures based on forward-looking assumptions that allocate the financial institution's aggregate risk appetite statement to business lines, legal entities as relevant, specific risk categories, concentrations, and as appropriate, other levels.	Clear metrics indicating when an operational disruption would present a risk: of harm to consumers or market participants; of harm to market integrity; to policyholder protection; to safety and soundness; or to financial stability. Limits are group-wide standards which guide underlying thresholds (e.g. align Recovery Time Objectives).
Assurance	Primarily delivered through monitoring MI on risk exposure with some periodic stress testing.	Primarily delivered through ongoing scenario testing of resilience.

A firm will implicitly, if not explicitly, consider its attitude to risk when setting impact tolerances, and in considering the nature of the severe and plausible scenarios it tests against. Impact tolerances should therefore be considered as complementary to (not alternative to, or replacing) a firm's existing risk appetite framework, and the supervisory authorities expect firms to be able to explain how the two interlink. Setting impact tolerances will require firms to review, and likely make changes to their existing risk appetite framework.

[22] Joint CP cover paper, section 3.6-3.7
[23] Taken from the FSB Principles for an Effective Risk Appetite Framework (link)
[24] The FSB chooses not to use the term 'risk tolerance'. For those bodies which refer to risk tolerance (e.g. Basel Committee on Banking Supervision) it is regarded as a more specific (often quantitative) determination of the boundaries of risk which the organisation is prepared to accept, whereas risk appetite tends to represent a desirable level of risk to take. The terms are sometimes used interchangeably.

Annex 2: How we help our clients

Using our unrivalled experience with clients on the topic of operational resilience, and our work helping regulators to develop proportional and effective regulation, we are strongly placed to help our clients with:

1 **Designing and building an operational resilience framework and toolkit**, including methodologies for identifying important business services and setting impact tolerances

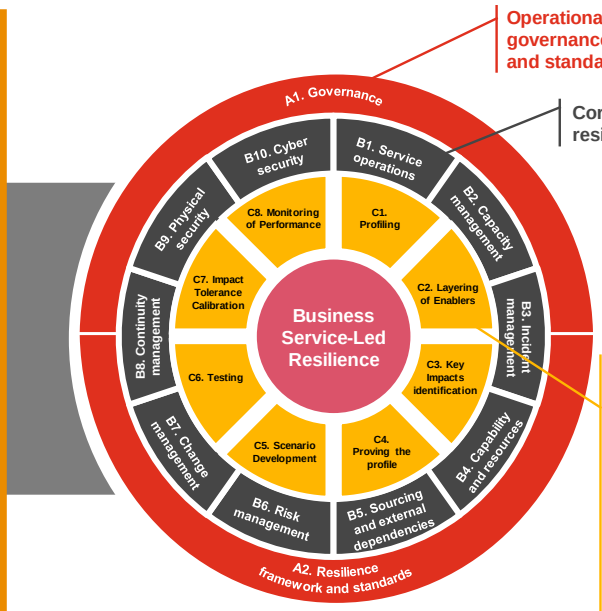
2 **Proactive assurance and maturity assessments** over the design, implementation and operation of their framework, including using our Operational Resilience Maturity Assessment

3 **Regulatory advice and consultation paper responses**, sharing our own insights on the evolving policy documents and through discussions with regulators and other firms.

Spotlight on Operational Resilience Maturity Assessment (ORMA)

In the five years since it was first introduced, ORMA has evolved with the regulatory expectations and the challenges the financial services industry has faced.

As of 2020, ORMA is in its third version. The two outer layers are traditional ORMA domains – however in this latest version we have added a 'business services' layer (innermost layer) to enable full front-to-back assessments of operational resilience capabilities.



Other PwC publications

- PwC Joint Report with TheCityUK: 'Operational resilience in financial service: time to act'.
- PwC guide to: 'Becoming operationally resilient'.

Our credentials include

- Invited to present oral evidence to the Treasury Select Committee for their inquiry into IT failures in 2019
- Are routinely selected by firms to conduct relevant Section 166 reviews for the PRA
- Are the provider of independent root cause analysis and post incident reviews to Boards following major operational incidents including the majority of high profile failures in recent years
- Run Operational Resilience Exchanges, bringing firms of similar business models together to share learnings on their approaches to define business services
- Supported the PRA in the development of Impact Tolerances in 2016.

Contributors

Simon Chard
Partner, Operational Resilience Lead

T: +44 (0) 7740 241051
E: simon.c.chard@pwc.com

James Maxwell
Partner

T: +44 (0) 7525 925982
E: james.maxwell@pwc.com

David Lukeman
Partner

T: +44 (0) 7801 227259
E: david.lukeman@pwc.com

David Bettesworth
Partner

T: +44 (0) 7764 958594
E: david.bettesworth@pwc.com

Duncan Scott
Director

T: +44 (0) 7894 393607
E: duncan.j.scott@pwc.com

Stella Nunn
Director

T: +44 (0) 7932 144627
E: stella.nunn@pwc.com

Stuart Birnie
Director

T: +44 (0) 7715 211440
E: stuart.m.birnie@pwc.com

Adam Stage
Senior Manager

T: +44 (0) 7483 422845
E: adam.stage@pwc.com

Notes