THE INSTITUTE OF OPERATIONAL RISK
An IRM Group Company

The England and Wales Chapter

Of the

Institute of Operational Risk

Comments on the

PRA (CP29/19) and FCA (CP19/32)
Consultation Papers on

Operational Resilience: Impact tolerances for important business services

6 September 2020

Dear PRA, FCA and the Bank of England

The England and Wales Chapter of the Institute of Operational Risk welcome and support the Bank of England, Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) proposals for stronger resilience for firms and financial market infrastructures (FMIs). The Chapter also welcome the opportunity to comment on the proposals as we have concerns about several aspects of them, which we feel will impair the benefit arising from the recommendations and impact implementation in firms.

We also welcome the co-operation and joint working between the authorities and would encourage the authorities to continue with this collaborative approach, including undertaking joint Operational Resilience reviews of firms and adopting a consistent approach wherever possible.

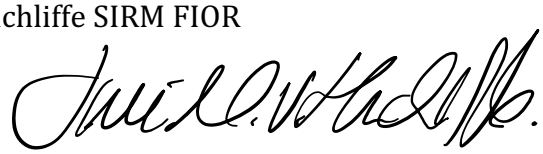
While the focus of the CPs has historically been on IT and Cyber threats, we recognize that the papers come at a time when Covid-19 presents a significant threat to Operational Resilience. As a result, we are pleased to note that setting an impact tolerance should enable firms to identify broader vulnerabilities and set resilience requirements for, amongst others, people. We would like to thank the PRA and FCA for extending the deadline for responses to 1 October to enable responses to be informed by the impact of the pandemic on Operational resilience.

The BCBS recently published a consultative document 'Principles for Operational Resilience' that addresses several of our concerns. We would therefore urge you to adjust the UK papers to reflect the Basel Committee's principles.

In the spirit of consistency, the Chapter has submitted the same response to the PRA and FCA. This includes, in section 4, a response to the 12 questions identified by the FCA. We would ask that the PRA also consider our responses to these questions as they address some of our concerns to the two CPs.

The Chapter would be happy to meet with the regulator to discuss our submission.

Dr Jimi M.V. Hinchliffe SIRM FIOR

Chairman 

Institute of Operational Risk
England and Wales Chapter

Index

List of Abbreviations

Abbreviation	Explanation
BCBS	Basel Committee on Banking Supervision
BCP	Business Continuity Plans
BIS	Bank for International Settlements
CP	Consultation Paper
CMORG	Cross Market Operational Resilience Group
CRO	Chief Risk Officer
E&W	England and Wales
FCA	Financial Conduct Authority
FMIs	Financial Market Infrastructures
FSI	Financial Stability Institute
IOR	Institute of Operational Risk
IRM	Institute of Risk Management
PRA	Prudential Regulation Authority
SMF	Senior Management Function

1. Introduction

The Institute of Operational Risk (IOR)** is the only institute solely dedicated to promoting the development and discipline of Operational Risk. The Institute:

- Is a global member-based organisation;
- Organises and delivers webinars and events;
- Develops Sound Practice Guidance papers (Risk Categorisation, External Loss Events, Key Risk Indicators, Operational Risk Governance, Risk Appetite, Risk Control Self-Assessment, Risk Culture and Scenarios);
- Undertakes research on emerging topics;
- Offers individuals the opportunity to take the Certificate in Operational Risk Management ('CORM').

There are two grades of membership available for personal applications:

- **Professional (PIOR):** a minimum of two years' relevant experience in risk management and working in an operational risk role or in a risk related role with a minimum of two year's practical experience (eg. Audit or Compliance);
- **Associate:** working towards achieving a higher grade of membership or actively engaged in risk management – generally at an early stage in a career in risk or a related discipline.

Corporate membership is also available, providing Corporate Members with the ability to allocate membership to a number of employees at a reduced cost, giving them access to all of the benefits of IOR membership.

The IOR is organised into Chapters across the globe, and the England and Wales (E&W) Chapter is chaired by Dr. Jimi Hinchliffe.

At its AGM on 22 May 2019, the IOR's members resolved that the Institute of Operational Risk join with the Institute of Risk Management Group. The IRM's prime objective is to provide education and training for the global risk management community and support the profession with cutting edge thought leadership. The IOR has the same and complementary purpose focused on operational risk.

Both organisations recognised that strong benefits and synergies could be achieved by coming together. The IOR and IRM are jointly committed to advancing the practice of operational risk management as we enter the fourth industrial revolution. The development of a global network of risk practitioners and professionals delivering value and service at a local and regional level is a key strategy of both the IRM and IOR. The IOR brand has been retained and will continue to represent excellence in the practice and profession of Operational Risk management.

---

* See https://www.ior-institute.org

A key element in the production of this response has involved consultation with our members. As a result, we have received feedback from the Fellows of the institute, consulted with members with considerable experience in this field and held a webinar to discuss the key concerns.

2. Executive Summary

While we welcome and support the proposals for stronger resilience for firms and FMIs the E&W Chapter of the IOR have identified a number of concerns that, if not addressed, may significantly impact the potential benefit of these measures. While comprehensive details of our concerns appear in section 3, we would like to identify below those areas that are of most concern:

- Without further clarification, the proposals could result in many firms establishing separate Operational Resilience silos, with a different duplicative risk framework and software. This further fragmentation of operational risk management and the creation of a new Operational Resilience *cottage industry*, is inefficient, will hinder the development of a holistic understanding of the firm's risk exposure, hinder the development of Operational Resilience and threaten the safety and soundness of firms;

- The proposals create ambiguity around the SMF 4 (CRO) and SMF24 (Chief Operations Officer) roles. This ambiguity could drive the creation of the siloed Operational Resilience frameworks mentioned above as both SMF functions seek to fulfil their responsibilities. To prevent this the supervisory authorities should clarify where responsibility for developing the policy, undertaking the self-assessment and exercising oversight and challenge should rest and the roles, interactions and cooperation expected between the first and second lines;

- The prospect of a single firm having two different impact tolerances is unlikely to prove beneficial and may generate confusion and misunderstanding within the firm. We would encourage the regulators to work closely together to harmonise the setting of impact tolerances for systemically important solo regulated firms;

- The collaborative approach demonstrated between the UK authorities should continue, including undertaking joint Operational Resilience reviews of firms and adopting a consistent approach wherever possible. This collaborative approach should be expanded to include the BCBS and other supervisors as regulatory activity on Operational Resilience expands;

- A more detailed explanation is needed of the requirement for PRA regulated firms to take into account public interest as part of their operational resilience framework and how the authority intends to assess and supervise this requirement;

- The industry should be encouraged to develop best practice including a range of impact tolerances, "generic" important business services and scenarios, which may be used by firms developing their Operational Resilience strategy.

3. Consultation Paper – Areas of Concern

The E&W Chapter of the IOR would like to raise the following concerns as a result of the CPs issued by the PRA (CP29/19) and FCA (CP19/32):

1. The relationship between Operational Resilience and Operational Risk

   Unfortunately, the CPs create ambiguity over the relationship between Operational Resilience and Operational Risk, and in parts the papers appear to propose that Operational Risk is a sub-component of Operational Resilience. Indeed, in figure 1 of CP 29/19 (page 3) Operational Risk Management is shown as supporting Operational Resilience.

   We are concerned that as a result firms will establish separate Operational Resilience silo's and that this can generate a lack of communication and understanding, creating barriers between the silos. This will repeat the mistake many firms made when seeking to manage conduct 'risks' including Financial Crime and Financial Compliance Risk. This resulted in different duplicative frameworks for Operational Risk, Financial Crime and Financial Compliance amongst others. In these instances each framework had a different approach to risk assessment (for example Risk and Control Self Assessments for Operational Risk, Compliance Risk Assessments for Financial Compliance and Risk Assessments for Financial Crime) and employed different software for managing the risks (the CeFPro Non-Financial Risk Leaders 2020 Survey shows the different software solutions for these three, and other, risk categories).

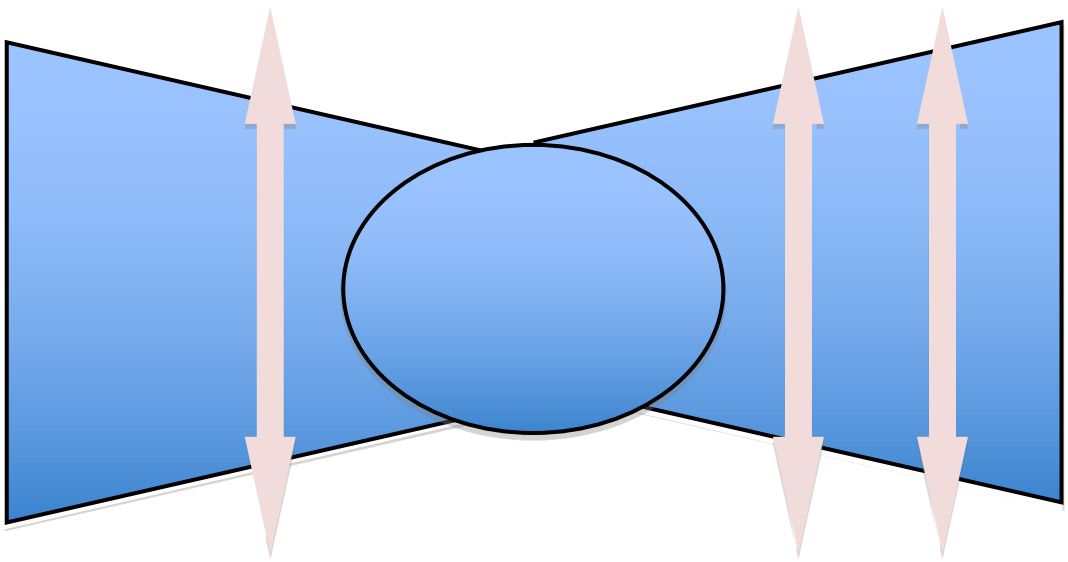
   The result is fragmentation, needless complexity, confusion, internal conflict and inefficiency, and as a consequence, it becomes difficult to obtain business line buy-in when they are faced with different risk silos effectively asking the same questions but in slightly different ways. In addition, the various software solutions are generally not capable of interacting, and firms are faced with comparing apples and pears, preventing the creation of a truly holistic understanding of the risks faced by the firm.

   Many firms have recognized the inherent weaknesses in previously establishing fragmented risk silos and are now seeking, often at some considerable cost, to align their risk functions (including Operational Risk, Compliance Risk, Conduct and Financial Crime Risk) to ensure improved risk management, a co-ordinated, collaborative and a holistic understanding of the firms risk exposure. This holistic view is usually developed under the umbrella of Operational Risk (sometimes rebranded as Non-Financial Risk). Moves towards a holistic approach are usually received favourably by supervisors.

   During a recent webinar we asked participants which approach they had adopted. About 15% stated that they had established separate Operational Resilience functions, while 45% had integrated the function into Operational Risk and 40% were still considering which approach is appropriate.

A firm's Operational Risk framework will seek to identify, assess, monitor, mitigate/manage and report the firm's risks. This is entirely consistent with capturing Operational Resilience as part of the overall Operational Risk framework. Many firms use the bow tie approach to understand their risks, and this may help illustrate our concern.

Figure 1: The Bow Tie



* Corrective controls include controls designed to adapt, respond to, and recover from operational events

The CP's recognition that Operational Resilience is an outcome, coupled with acceptance that Operational Resilience includes the ability of firms to **prevent**, adapt, respond to, recover and learn from operational disruptions, demonstrates that Operational Resilience should be seen as a component of Operational Risk leveraging existing building blocks, rather than vice-versa. The bow tie approach, and the recognition that events will occur, places the CP proposals on the impact side of the bow tie. Operational Resilience can therefore be seen as a component of Operational Risk, indeed the Operational Risk framework is applied at the cause and event stage, including event investigations and lessons learned. The Operational Resilience approach is certainly an improvement on the ways in which impacts are managed within Operational Risk and instead of significantly enhancing existing Operational Risk Frameworks and strengthening risk management within firms, the CP proposals are presenting Operational Resilience as a separate discipline and threatening to weaken the risk

management process thereby threatening the statutory objectives of the supervisory authorities.

An additional consideration is the relationship between Operational Resilience and Business Continuity. In many firms, responsibility for Business Continuity rests with the Operational Risk function, strengthening the case for Operational Resilience to be seen as a component of Operational Risk. As firm's continue to evolve their response to the pandemic it is possible that distinguishing between the Business Continuity and the Operational Resilience may be inefficient and impact incident responses. Many incidents will begin as continuity events with a single point of failure before morphing into a resilience event. This suggests that firms could benefit considerably from considering Business Continuity and Operational Resilience in unison.

Covid 19 has emphasised the importance of Operational Resilience being a component of Operational Risk, together with Business Continuity. The organisations that are faring best during the crisis are those who maintain their Operational Resilience and Business Continuity frameworks under the Operational Risk umbrella, enabling them to undertake a unified response to developments.

We also note that the BCBS Consultative Document 'Principles for Operational Resilience' recognises the benefits that effective management of operational risk can bring and would argue that this supports the suggestion the authorities should rethink their view of the relationship between operational resilience and operational risk. For example:

- Principle 1 : 'Banks should utilise their existing governance structure to establish, oversee and implement an effective operational resilience approach that enables them to respond and adapt to, as well as recover and learn from, disruptive events in order to minimise their impact on delivering critical operations through disruption';

- Principle 2 : 'Banks should leverage their respective functions for the management of operational risk to identify external and internal threats and potential failures in people, processes and systems on an ongoing basis, promptly assess the vulnerabilities of critical operations and manage the resulting risks in accordance with their operational resilience expectations.'

We feel a clear reflection of the BCBS principles in the authorities' approach would prove useful in the UK.

2. Interaction with other management responsibilities

The CPs ambiguity with regard to the relationship with the Operational Risk function is increased by the ambiguity surrounding the role of the Senior Management Function SMF24 (Chief Operations Function) and the SMF 4

(Chief Risk Function). In an environment where these individuals can be held accountable for their actions, this lack of clarity is at best unhelpful.

The papers give the SMF 24, where it applies, overall responsibility for implementing Operational Resilience policies and reporting to the Board. This effectively makes the SMF 24 the impact owner. While day to day responsibility for implementation sits with the first line the paper does not mention the interactions and cooperation expected between the first and second lines or make it clear where responsibility should rest for developing the policy, undertaking the self-assessment and exercising oversight and challenge. Recognising the need for the involvement of an independent party in Operational Resilience and adopting the approach used for Operational Risk, these responsibilities should rest in the second line with the Risk Function.

Clarifying the relationship between the SMF 4 and SMF 24 will avoid ambiguity and also reduce the risk of the SMF24 creating a separate resilience framework which largely duplicates other existing risk frameworks.

Our recent webinar reflected this ambiguity with about 30% of participants stating that the COO is leading the resilience initiative while another 30% responded that the CRO is leading the initiative. The remaining 40% of participants noted that the initiative is being led jointly by the COO and CFO.

3. Impact Tolerances and Dual Regulated Firms

The CPs propose that a firm regulated by both the PRA and FCA could have up to two impact tolerances for each important business service – one considering financial stability, safety and soundness and policy holder protection, the other set with reference to consumer harm and harm to market integrity. We feel the prospect of a single firm having two different impact tolerances is unlikely to prove beneficial and may generate confusion and misunderstanding within the firm. It would seem more effective if the lowest tolerance was applied across the firm. This would seem to be recognised in the PRA CP which states 'it may be appropriate for firms to focus on the impact tolerance which has the shortest duration when prioritising actions.' However, it would be helpful if this could be expanded upon to clarify 'when' it would be appropriate for firms to focus on the tolerance with the shortest duration.

4. Dual Regulated Entities

For dual regulated firms there is the possibility that a non-joined up approach on regulation between the PRA and FCA will lead to significant but unnecessary duplication of effort and burden within a firm preparing for visits, providing information and approaching the visits.

We recommend the collaborative approach demonstrated between the UK authorities to date should continue including undertaking joint Operational Resilience reviews of firms and adopting a consistent approach wherever possible. As expanded upon later this collaborative approach should be expanded upon to include the BCBS and other supervisors as regulatory activity on Operational Resilience expands.

5. Scenario Testing

Scenario testing is a key element of Operational Resilience and many firms already undertake scenarios as part of their Operational Risk Framework. We would hope that firms will utilise existing scenario capabilities to undertake this important function, rather than establishing an Operational Resilience Scenario function.

While the supervisory authorities do not currently set scenarios, we would urge them to do so, establishing a set of core severe but plausible operational scenarios all regulated entities must perform. While this would benefit all firms, we feel it would be particularly beneficial for small firms. In addition, the response to the 2020 pandemic would have been significantly improved if the supervisory authorities had mandated a core pandemic scenario (also see section 4: Covid 19 and Operational Resilience).

6. Mapping

Mapping has proved difficult for many firms and is often extremely resource intensive. We recommend that the supervisory authorities should provide further clarification and set minimum standards for mapping as we feel this would be particularly beneficial for small firms. Publishing some forms of examples for good practice and poor practice would increase the chances of firms putting in place a process that is both consistent and in line with the regulator's thinking.

7. Public Interest

The PRA's Draft Supervisory Statement introduces the concept of public interest when making investment decisions with regard to a firm's Operational Resilience (page 62). We would appreciate a more detailed explanation of the need for PRA regulated firms to take into account public interest as part of their operational resilience framework and how the authority intends to assess and supervise this requirement.

8. Proportionality

The papers recognize that there is a need for a proportionate minimum standard of Operational Resilience, and much is made within the papers of the importance of proportionality. For example, CP29/19 states that:

- 'Firms should document their mapping in a way proportionate to their size, scale and complexity' (page 12, paragraph 4.15);
- 'The nature and frequency of a firm's testing should be proportionate to its size and complexity' (page 13, paragraph 4.19);
- 'Larger and more complex firms are expected to identify more important business services than smaller and simpler firms. The latter will therefore have less work to perform not only around identifying important business services but also around setting impact tolerances, mapping and testing them' (page 20, paragraph 6.19).

In addition, CP 19/32 states that:

- 'We propose to apply the proposals in this CP proportionately to firms reflecting the impact on consumers and market integrity if their services are disrupted' (page 6, paragraph 2.6);
- 'Firms should structure oversight of operational resilience in a way that is effective and proportionate for their business' (page 27, paragraph 7.9);
- 'Our approach is risk-based and proportionate considering the nature, scale and complexity of a firm's operations' (page 32, paragraph 8.10).

The comment on page 20 of CP29/19 could be interpreted as implying that for small firms, proportionality is simply a reflection of the number of important business services. This could be taken to mean that every firm must undertake an identical Operational Resilience process for each business service, irrespective of the nature, scale and complexity of the firm. As a result, we feel firms, particularly smaller firms, would benefit from a more detailed explanation of how proportionality will apply to them and impact their Operational Resilience frameworks.

9. Industry Engagement

We are pleased to note that the supervisory authorities will engage with firms and FMIs through a combination of round tables discussions, industry fora, speeches and more focused group discussion. In the past the supervisory authorities have created working groups for specific risks. The minutes of these groups have been published along with details of the industry membership.

We would like therefore to commend the creation of the Cross Market Operational Resilience Group (CMORG) jointly chaired by the Bank and UK Finance with participants from 29 of the most systemically important firms and Financial Market Infrastructures. Nevertheless, we recommend that another PRA/FCA Operational Resilience working group be established with industry members from a wider cross section of firms and industry bodies, including small firms. This would help provide a consistent mechanism for the supervisory authorities to gain information on the Operational Resilience implementation process industry wide and resolve issues quickly. Through this mechanism or separately, the industry could be encouraged to

develop best practice including a range of impact tolerances, "generic" important business services and scenarios. Needless to say, we would be very happy to be part of such a group.

10. International Regulatory Convergence

The UK Authorities have chosen to publish their detailed proposals in advance of the BCBS Consultative Document 'Principles for Operational Resilience', which were published in August 2020. We suggest that as a result of front-running the publication of the international policy on Operational Resilience, the UK should now revise their proposals to bring them in line with the international standards. Following the Global Financial Crisis, the UK authorities chose to front-run the international standards (BCBS and from the EU) in a number of areas, which meant they had to revise their policies once the international standards caught-up. This was not only inefficient, imposing unnecessary costs of compliance on firms, but also creates additional operational risks as firms have to run additional change programmes to meet the revised rules. The E&W Chapter of the IOR encourage the UK authorities to ensure that their proposals are fully in-line with the recently published international BCBS principles for operational resilience, before they finalise and implement them in the UK, and to be mindful of avoiding contributing to further fragmentation of the global regulatory architecture.

We note that the UK papers speak in terms of the importance of '*Important Business Services*' while the BCBS talks of '*Critical Operations*'. Our members would welcome an understanding of the significance, if any, of these two different terms.

We also encourage the UK authorities to be cognisant of the impact of their proposals and the manner in which they are implemented (especially in relation to the calibration of impact tolerances) on the position of the UK as a major financial centre. Post-Brexit, the UK is more directly in competition with New York, but also more able to compete with New York in relation to UK regulatory policy (as it is no longer bound by the EU regulations). The UK authorities should monitor carefully what the U.S. authorities plan to do on Operational Resilience, and ensure they do not significantly disadvantage the UK market and UK institutions by imposing more stringent requirements than in their main competitor market.

11. Service Providers Tolerance vs. Firm Tolerance

The CPs propose that firms regulated solely by the PRA or FCA will set impact tolerances for each important business service based upon different criteria – one considering financial stability, safety and soundness and policy holder protection, the other set with reference to consumer harm and harm to market integrity.

There will be occasions when an FCA regulated firm will be dependent on important services provided by a PRA regulated firm to deliver one or more of its own important business services. An example of this would be an FCA regulated bank identifying payments to customers as an important business service which requires the service provided by a PRA regulated FMI. In this case the FCA regulated bank will have a regulatory objective to meet which would rely on the PRA regulated firm potentially making a commercial decision on the resilience of the service if they set a PRA led tolerance greater than that of the bank.

To avoid such commercial conflicts arising we would encourage the regulators to work closely together to harmonise the setting of impact tolerances for systemically important solo regulated firms. Industry would benefit from the development and publication of a range of impact tolerances.

12. Unintended Consequences

We urge the UK authorities to be mindful of possible unintended consequences of their proposals, particularly if they are not implemented with care and proportionality. For instance, it is possible that faced with significant additional costs of increasing operational resilience in relation to a particular Important Business Service, a firm may take a commercial decision that they will no longer provide the business service. This may have the effect of negatively impacting consumers who relied on the service, reducing choice and have anti-competitive effects, leading to higher prices.

We also urge the authorities to be sensitive to the pressures many firms are already under to reduce costs in order to maintain the viability of their business models and the likely costs of meeting the requirements. Firms have been confronted by a double whammy of extremely difficult market conditions and higher regulatory capital requirements, and the new requirements for Operational Resilience are likely to require significant spend, especially in relation to systems. We urge the Authorities to be proportionate and ensure that efforts to increase Operational Resilience do not have the perverse effect of threatening firm safety and soundness.

4. Covid 19 and Operational Resilience

The coronavirus pandemic of 2020 has effectively stress tested firm's Operational Resilience frameworks and raises a number of interesting considerations. Before the virus emerged, the focus of Operational Resilience had been almost solely on cyber and IT and the duration of any event was significantly shorter than experienced by the pandemic. The Supervisory Authorities and firms will now need to ensure their resilience frameworks include the availability of all necessary resources, including the possibility of more than one resilience event occurring simultaneously. For example:

- People – Many Operational Resilience frameworks assume that human resources will be available to mitigate IT issues. This may not always be the case;

- Systems/Digital – In order for staff to work from home to the extent required, many firms and the regulators had to enhance their digital capabilities for both staff, customers and regulated entities. All parties must be able to demonstrate the adequacy of their digital capabilities;

- Buildings – The emphasis of many Business Continuity Plans (BCP) has been on ensuring the availability of buildings, with continuity sites used to mitigate this risk. One consequence of the pandemic has been that while buildings remained available it was not possible to use them.

This is in keeping with the BIS FSI brief number 2 issued in April 2020 which suggested that international efforts to come up with operational resilience standards should take into account at least the following: Critical/essential employees; IT infrastructure; Third-party service providers, and; Cyber resilience.

The pandemic has also highlighted a concern at the extent the Operational Resilience proposals focus on impact. The wide variety of causes require very different responses and the proposals should be expanded to reflect this concern.

A key element of the Operational Resilience proposals is the requirement for firms to test themselves against severe but plausible operational scenarios to identify and address vulnerabilities. It is therefore important to understand whether the coronavirus pandemic of 2020 reflected a severe but plausible operational scenario (perhaps in the form of a Gray Rhino - a highly probable, high impact yet neglected threat) or lay outside the realm of regular expectations (Black Swan). In addition, we must ask if the pandemic could have been captured as part of the risk identification component of firms Operational Risk frameworks, perhaps within the RCSA process, within the general scenario process or as part of the top and emerging risks.

If the pandemic was a Black Swan, it could be argued that firms and regulators can claim they could not test themselves against a pandemic. If the scenario could not have been predicted, only preventative and generic detective controls could have been established. If it is not a Black Swan, then deficiencies in the risk management

framework prevented the event from being identified and managed/mitigated. In this case these deficiencies must be addressed to ensure that firms do not fail to test themselves against a severe but plausible pandemic scenario, that they prepare for and mitigate similar events and that specific preventative, detective and corrective controls are put in place.

Black Swan or Gray Rhino?

Some observers suggested that the world experienced a Black Swan event. However Black Swans have three attributes, the event:

- Is an outlier as it lies outside the realm of regular expectation because nothing in the past can convincingly point to its possibility;
- Carries an extreme impact;
- In spite of its outlier status, human nature makes us concoct explanations after the fact making it explainable and predictable.

Given these attributes it is important to understand whether the Covid 19 pandemic lies outside the realm of regular expectations. Clearly the evidence shows it was not, including:

- Three worldwide outbreaks of influenza occurred in 1918, 1957 and 1968, with 1918 worldwide deaths estimated to be at least 50 million;
- Severe Acute Respiratory Syndrome (SARS) – This is a species of coronavirus and caused outbreaks of severe respiratory diseases in humans in 2002 and 2003, killing almost 800;
- The Western African Ebola virus epidemic in 2013-2016 was the most widespread outbreak of Ebola Virus Disease (EVD). The current Ebola outbreak began in 2018.

As the pandemic does not lie outside the realm of regular expectations the pandemic should have been envisaged as part of the risk identification component of firms Operational Risk frameworks and should have been the subject of a severe but plausible operational scenario to identify and address vulnerabilities.

Some commentators have therefore described the pandemic as a 'Gray Rhino'[1] - a highly probable, high impact yet neglected threat. Gray Rhinos are not random surprises but occur after a series of warnings and visible evidence and their identification could be an important outcome of the operational resilience process.

[1] The Gray Rhino: How to Recognise and Act on Obvious Dangers We Ignore by Michele Wucker (Published 2016)

5. Responses to the Questions in the FCA paper

The FCA Consultation Paper contains a number of questions. The responses of the E&W Chapter of the IOR are shown below:

Q1: Do you agree with our proposal for firms to identify their important business services? If not, please explain why.

We agree.

Q2: Do you agree with our proposed guidance on identifying important business services? Are there any other factors for firms to consider?

While we appreciate the value of the guidance provided in the CP, we feel that many firms, particularly smaller firms, would benefit from further elaboration of additional factors, perhaps for example possible impact on other firms. There is a potential concern that publication of the new requirements will be followed by supervisory visits that evaluate firms against a set of criteria that were not shared with the firms originally. We feel that a better outcome will result from additional guidance on identifying important business services.

Q3: Do you agree with our proposals for firms to set impact tolerances? If not, please explain why.

We agree, although we hope the supervisory authorities will recognise the difficulty associated with this task.

Q4: Do you agree that duration (time) should always be used as 1 of the metrics in setting impact tolerances? Are there any other metrics that should also be mandatory?

We are unable to identify an instance where duration would not be an important impact tolerance metric and agree that it should therefore always be used. However, we also recognise that other metrics can also be identified and that these could take precedence over duration. For example, a firm could have a metric for duration and the number of customers impacted. In the event that only a very small proportion of the potentially impacted customers are affected, the duration of any outage could be seen as less important.

Q5: Do you agree with our proposal for dual-regulated firms to set up to 2 impact tolerances and solo-regulated firms to set 1 impact tolerance per important business service?

The CPs propose that a firm regulated by both the PRA and FCA could have up to two impact tolerances for each important business service – one considering financial stability, safety and soundness and policy

holder protection, the other set with reference to consumer harm and harm to market integrity.

We find the prospect of a single firm having two different impact tolerances is unlikely to prove beneficial and may generate confusion and misunderstanding within the firm. It would seem more effective if the lowest tolerance was applied across the firm. This would seem to be recognised in the PRA CP which states 'it may be appropriate for firms to focus on the impact tolerance which has the shortest duration when prioritising actions'.

Q6: Do you have any comments on our proposed transitional arrangements?

We support the proposal to give firms time to ensure that they can take the actions necessary to improve their operational resilience. Nevertheless, we recognise that some firms will experience difficulty with some aspects of the Operational Resilience requirements, mapping and IT infrastructure for example, and this may make the 3 year deadline difficult to achieve for some firms. We hope that the supervisory authorities will take into account the implementation steps taken and any considerations the firm cannot control when reviewing firms that fail to meet the deadline.

We also note that firms authorised within the transitional period will have to comply with the requirements on deadline day. This could act as a barrier to entry, negatively impacting competition and leading to less choice, higher prices and customer harm, and we would hope that the supervisory authorities will exercise discretion when dealing with new market entrants.

Q7: Do you agree with our proposed approach to mapping? If not, please explain why.

Mapping has proved difficult for many firms and is often extremely resource intensive. We recommend that the supervisory authorities should set minimum standards for mapping based on the desired outcome (i.e. identification of resource vulnerabilities) and feel this would be particularly beneficial for small firms.

Q8: Do you agree with our proposed approach to testing? If not, please explain why.

Scenario testing is a key element of Operational Resilience and many firms already undertake scenarios as part of their Operational risk Framework. We would hope that firm's will utilise existing scenario capabilities to undertake this important function, rather than establishing a duplicative Operational Resilience Scenario function as many other aspects of non-financial testing and scenario analysis

currently exist (e.g. cyber security, business continuity, incident management) and these may be leveraged in the assessment of Operational Resilience.

While the supervisory authorities do not currently set scenarios, we would urge them to do so. While this will benefit all firms, we feel it would be particularly beneficial for small firms.

Q9: Do you agree with our proposals for communication plans? If not, please explain why.

We agree with the proposals for communication plans. Operational disruptions have shown the importance of effective communication. Firms already have communication plans as part of their Business Continuity Plans (BCP) and we would hope that experience and knowledge gained in developing BCP communication plans will be applied for Operational Resilience.

Q10: Do you have any comments on our proposed requirement for a self-assessment document?

The paper does not make it clear where responsibility should rest for undertaking the self-assessment. Recognising the need for the involvement of an independent party to undertake the self-assessment and adopting the approach used for Operational Risk, these responsibilities should rest in the second line with the Risk Function.

Q11: Do you have any comments on the cost benefit analysis?

No comment.

Q12: Do you have any comments on the examples of existing legislation?

No comment.