CAPCO

MANAGING THE INEVITABLE

A PRIMER ON OPERATIONAL RESILIENCE

TABLE OF CONTENTS

MANAGING THE INEVITABLE: A PRIMER ON OPERATIONAL RESILIENCE

As events show, the phrase 'expect the unexpected' is good advice. Over the past few years, there have been many events which we could not easily predict, yet in hindsight seemed inevitable – from large scale cyber attacks, data outages and supplier process failures, to disrupted commutes, terror incidents and extreme natural disasters. While there is no link between these occurrences, they typically have one thing in common. They have all, to varying degrees, disrupted financial services firms' ability to provide their customers with an expected level of service.

The financial ecosystem is becoming more complex with greater outsourcing, more use of cloud computing and fintechs operating at more points within the value chain, all increasing the opportunities for disruption to services at the same time as enhanced expectations from customers and regulators alike. Operational resilience is the response to this. The underlying assumption behind operational resilience is that events will occur and that the response needs to be planned and managed once the inevitable happens. It is no longer a question of 'if' but 'when'.

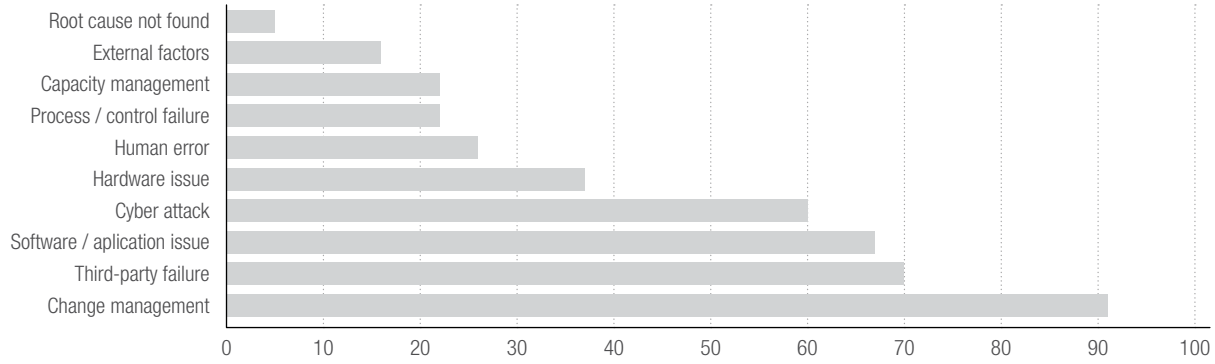
The definition of operational resilience[1] used by UK regulators is:

- 'The ability to prevent, adapt, respond to, recover and learn from disruptions to better serve customers and, more broadly, ensure financial stability'.

This well describes the end-to-end nature of the topic well as well as bringing out that it is a process in its own right.

It differs from operational risk in assuming that events will happen and require a response rather than measuring control effectiveness and quantifying potential losses. It is more focused on the broad impact on customers and financial stability than continuity of business (CoB)and operational continuity in resolution (OCIR).

Operational resilience should not be seen as a one-off exercise but rather a consideration that should be embedded in how a firm operates, and in all decision-making. The analysis needs to be refreshed regularly and the response to potential events rehearsed on a frequent basis. It would also be wrong to assume that operational resilience revolves primarily around cyber threats; most service disruptions are caused by internal problems such as the issues around the TSB data migration in 2018 following its sale from Lloyds to Sabadell[2]. The chart below shows the number of disruptions reported to the FCA in 2017 and 2018 by type.



Overview of technology outages report to the FCA (2017 – 2018)

Source: Financial Conduct Authority. "Cyber and technology resilience: themes from cross-sector survey 2017 – 2018", November 2018)

1. https://publications.parliament.uk/pa/cm201919/cmselect/cmtreasy/224/224.pdf
2. https://uk.reuters.com/article/uk-tsb-report/tsb-and-parent-sabadell-heavily-criticised-for-it-crash-that-locked-2-million-out-of-accounts-idUKKBN1XT176

MANAGING THE INEVITABLE: A PRIMER ON OPERATIONAL RESILIENCE (CONTINUED)

While the responsibility for a firm's resilience framework rests, under the UK Senior Managers and Certification Regime (SM&CR), with the SMF24 Chief Operations Function, the ultimate responsibility lies with boards and senior managers and they should be familiar with and sign off the approach as part of the annual self-certification process.

For most firms, many of the elements required to ensure operational resilience already exist to some degree. What has changed is that UK financial regulators have, following an extensive consultation exercise, defined the steps that they expect firms they regulate to undertake to ensure that their operations are resilient.

Both the UK FCA and PRA published final consultation papers on the topic in December 2019, stating that they expect to publish formal regulations mandating these steps in late 2020 for implementation over the following three years. While the principle of proportionality will apply, this is more evident in the sense of urgency expected and the impact tolerances placed on a firm's business operations rather than omitting any element.

With the PRA focused on systemic issues and the FCA concerned with the impact on customers, the latter will typically expect a lower impact threshold.

The two consultation papers can be found here for the PRA[3] and here for the FCA[4]. Both papers adopt the same approach in terms of the steps that they expect regulated firms to take. We detail these steps in this paper as they represent a logical approach and will, in all likelihood, be the ones that will need to be undertaken.

There are practical reasons for not waiting to the end of the three-year period in 2023 to have completed preparations. There is undoubtedly a competitive advantage in adopting this approach to operational resilience ahead of peers in being able to demonstrably better serve customers. If they themselves are regulated they will also be looking for the outcome of their suppliers' self-assessments as part of their own operational resilience preparations in advance of the deadline.

There will also inevitably come a point, ahead of the deadline, that the new standard becomes the market expectation with negative consequences for those firms who have not yet adopted this approach to operational resilience. In addition, service disruptions cost significant amounts of value both in terms of direct compensation and potential fines and, more importantly, the impact on customer trust. This is all on top of just building a better business for the sake of it. It makes sense to be ahead of the pack.

3. https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/cp2919.pdf
4. https://www.fca.org.uk/publications/consultation-papers/cp-19-32-building-operational-resilience-impact-tolerances-important-business-services

OPERATIONAL RESILIENCE: A COHERENT APPROACH

There are three distinct phases to operational resilience:

1. **Preparing for the inevitable.**
   This drives the bulk of the task and involves really understanding the underlying dynamics of key business processes, their vulnerabilities and then testing how they respond to simulated events. The step by step approach taken by the regulators breaks this down into a logical series of actions.,
2. **Managing the response.**
   The success or otherwise in responding to an event will be determined by the thoroughness of the steps taken beforehand around training, governance, communications and setting up the physical/informational arrangements to manage the response
3. **Learning lessons.**
   Processes and procedures need to be reviewed in light of events that have impacted the firm or other organizations to ensure that the approach to resilience is still sound and that the firm can stay within its impact tolerances.

PREPARING FOR THE INEVITABLE

Identification of important business services. The starting point is identifying the important business services which a firm delivers to its customers and, by extension in some circumstances, the market. These are specific, viewed from a customer perspective and include items like making an annuity payment, making correspondent banking payments, providing account balances, selling or buying equities, customer authentication (that is the gateway to providing further services) and the suchlike. They are not internal systems such as a general ledger, HR database or business lines such as mortgages or foreign exchange, nor are they internal systems such as the HR salary system.

Definition of impact tolerances. For each important business service, a measurable level of disruption should be defined within firms as the maximum that is tolerable to customers who use the service. The Impact tolerances should be in terms of the impact on clients and also the broader market, if relevant. Impact tolerances should take into account relevant factors such as the number of customers effected and financial loss to them, duration of the disruption, data integrity, substitutability, time of day, impact on market stability etc.

Once defined, it is the impact tolerance for each of these services that sets the limit that management must take steps to ensure is not exceeded. Remaining within impact tolerances will be the key measure by which the success of a firm's approach to resilience is measured. This will have the effect of focusing senior managers and boards on the steps necessary to ensure that firms meet regulations such as prioritizing spend on changes to IT infrastructure. Firms regulated by both the FCA and PRA may have different impact tolerances due to meet the focus of each regulator.

PREPARING FOR THE INEVITABLE (CONTINUED)

Mapping.
To be able to understand the potential points of disruption to a process it first needs to be mapped. Parameters such as timing should be added to the information flows between the components of the processes that deliver all a firm's important business services. There is a careful balance to be drawn between going into too greater detail and capturing the points in a process that potentially could cause disruption. There is no need to include the mapping documentation into the annual self-certification.

Third-party service providers.
With the developments in the provision of financial services and how financial companies are structured leading to increased use of suppliers in key processes, e.g. FMIs, fintechs, cloud computing, there is a growing recognition that resilience extends beyond the traditional boundaries of a firm. There is also an awareness that the provision of services to the market by a limited number of suppliers may itself create concentration risk.

To address this, the EBA is recommending the creation of a 'register of outsourcing'[5] for each firm that, while not necessarily public should be readily available to regulators and stakeholders and include, for critical or important services, detailed information on suppliers. Firms need to be satisfied that their suppliers have put in place appropriate steps to ensure that they can continue to deliver the service they provide in light of disruption. It is expected that this will take the form of reviewing a firm's operational resilience self-assessment where the supplier is a regulated firm. Where the firm is not regulated a similar level of rigor should be expected.

Vulnerability assessment.
With the key elements of a process mapped and third parties identified, a thorough review of the vulnerabilities at each step of the process can be undertaken. Some of these will be more general than others (terrorist attack or natural disaster versus EUC host platform failure). All aspects should be taken into account, not just technology but also factors such as dependency on key individuals and single points of failure. A good example[6] is the Crypto exchange CEO who died along with his passwords.

Vulnerability remediation.
Once vulnerabilities have been identified then the necessary resources should be put against removing each one to the point at that the process can be managed so as to not exceed the defined impact tolerance if an event occurs. This may lead to the acceleration of system replacement as the cost of addressing specific vulnerabilities is uneconomic compared with that of simply replacing legacy architecture. This is also an opportunity to simplify systems into a more customer centric model that is better suited to a world of APIs and increasing integration with suppliers.

The opportunity should also be taken to improve the MIS that is generated on a firm's process performance and status. Once the approach to resilience is embedded it can be designed into systems from inception at little additional cost. Embedding resilience will also involve training individuals responsible for process design and implementation to ensure that good practice is followed and reduce the need for subsequent remediation.

Scenario testing.
To ensure that impact tolerances are not exceeded given an event a number of plausible scenarios should be run through rigorously to identify each one's impact on the Important Business System (IBS). While the regulators will not specify the scenarios that should be considered, their emphasis is both on plausible as well as severe events; they fully realize that there are some theoretically possible scenarios or combination of scenarios would cause an impact tolerance to be breached. Scenario testing should be a part of the annual self-certification process.

5. https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA revised Guidelines on outsourcing arrangements.pdf
6. https://abcnews.go.com/Business/company-loses-190-million-cryptocurrency-ceo-dies-sole/story?id=60851760

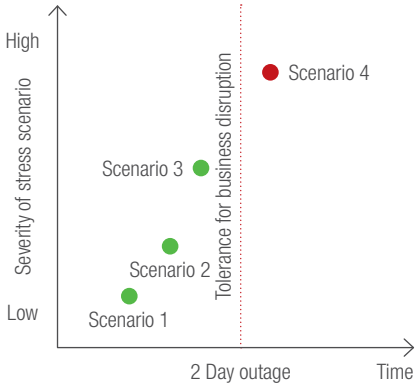
PREPARING FOR THE INEVITABLE (CONTINUED)

Self-assessment.
The relevant senior managers and board should sign off that their firm can remain within its impact tolerances given disruption to its processes, detailing the important business services, the relevant impact tolerances, third-party dependencies as well as the results from the scenario testing. There is no need to describe the processes and mapping in detail. It should, however, talk to the reasoning behind the assessment that the firm is operationally resilient.

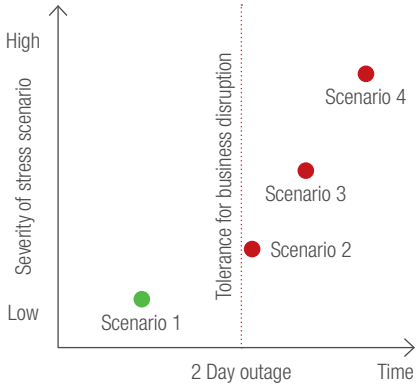
Annual review.
While changes to processes should be made as soon as the need is identified (e.g. due to an event that has happened at a competitor) all the steps covered already should be reviewed on at least an annual basis to identify any changes and drive remediation. One key element is using scenario testing to prove that the firm can remain within its impact tolerances given disruption to its processes. This should all culminate in a new self-assessment document signed off by the relevant senior manager and board.

Some scenarios would see impact tolerances being exceeded

Case one: A firm considers its impact tolerance against severe but plausible scenarios. Operation resilience is sufficient – it is disproportionate to expect the firm not to breach its impact tolerance in the extreme scenario of scenario 4.



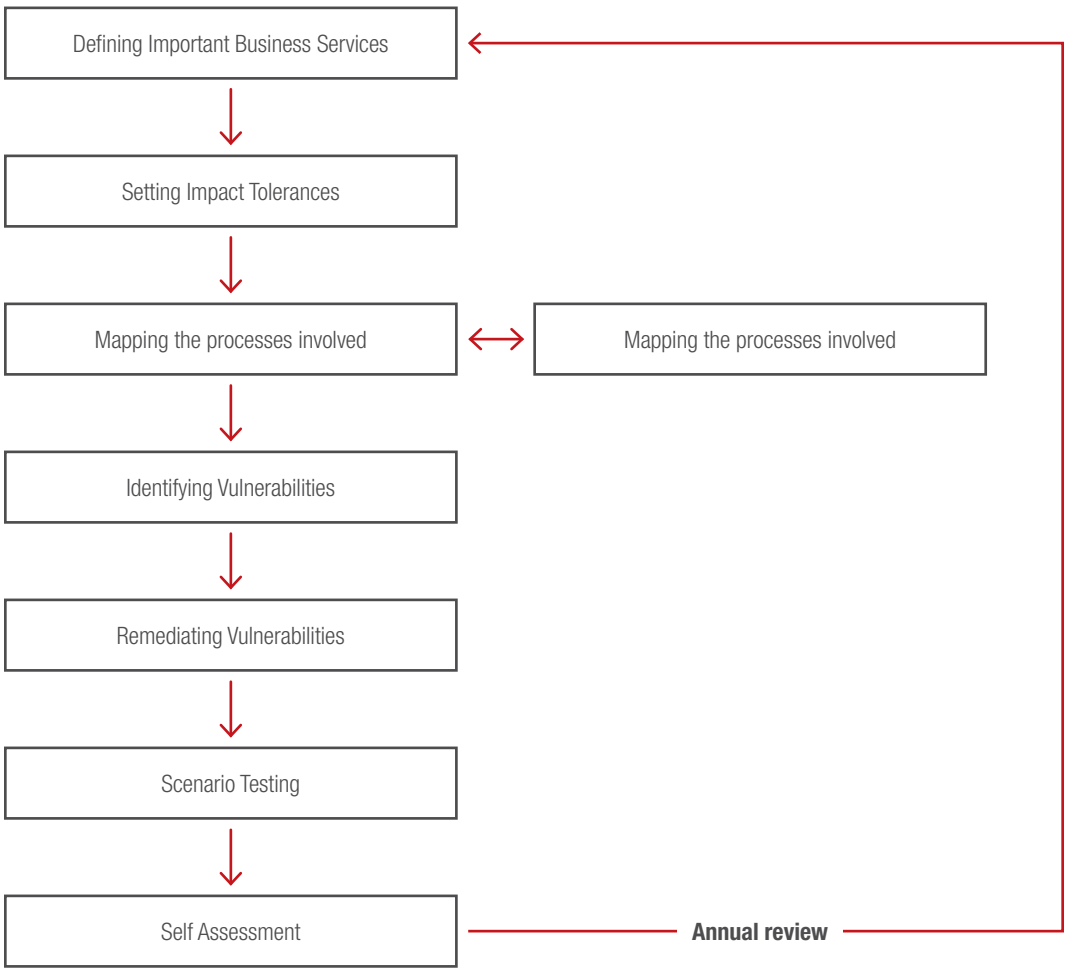
Case two: A firm considers its impact tolerance against severe but plausible scenarios. In this cas, operational resilience is not sufficient – the firm should take steps to improve operation resilience.



Scenario **recovered** within tolerance

Scenario **not recovered** within tolerance

Some scenarios would see impact tolerances being exceeded



MANAGING THE RESPONSE

> *Every battle is won before it is fought.*
>
> Sun Tzu – The Art of War

This quote is as true of responding to an event today as it was when written 2,500 years ago. Once an event is underway the training of the individuals involved in managing the response as well as the structures put in place beforehand will determine how successfully a firm responds to the challenge. There will not be time to extemporize a well-founded response.

Identifying the right decision-making body and the freedom and constraints of their decision-making is the starting point. Too small and it is not representative of all relevant stakeholders while too large and it becomes paralysed and unwieldy. Who is ultimately the responsible for decision making and what influence can other members of the forum exert? The factors that determine the answers to these are largely firm specific but all individuals will need to be trained. Whatever arrangements are adopted should fully meet the UK SM&CR standard.

Training should include the nature of some possible disruptions such as the types of cyber threat and as well as the end to end processes for the business to enable better discussion and challenge when the inevitable happens. More importantly, it should cover and rehearse decision-making in fast paced environments based on incomplete information. This is typically very different to normal decision-making due not only to the compressed timeframe but also to the much greater number of variables. (e.g. a trader may face having to make a choice in a similar timeframe but will typically face binary decisions – whether to go long or short).

Information is not only key but will also likely be more fragmented making the creation of a picture of the situation far harder. Information needs to be filtered and presented in a way that allows executives to make the best decisions possible and remain focused on the more critical items.

This MIS on process performance should be designed in from system inception and allow for rapid aggregation. Best practice would be where the CHAPS interface sends a confirmation to a central dashboard that the daily feed has been sent (and received at the other end). Information on the firm's processes, the status of those processes needs to be readily available and visualized in a way that facilitates understanding. SMEs should also be available to support decision making.

Communications is a key element in managing the response, critically to customers but also internally, to regulators and potentially other market participants.

Firms should look to create a central control point through which information and decision making is channeled and tracked.

Practice makes perfect and all elements of the event response apparatus need to be rehearsed regularly in response to simulated events to be effective. After each rehearsal a thorough review should be held to identify any issues.

Efforts should be made to learn from non-financial organizations such as the UK Armed Forces and emergency services who are experienced in decision-making in fast moving situations to ensure that best practice is adopted. One approach used by many western militaries is the concept of the OODA loop[7]. This is a way of breaking down the response to fast moving situations into phases that then allows each one to be focused on and accelerated leading to dominance on the battlefield. This can be adapted to managing a response in an operational resilience context.

7. https://en.wikipedia.org/wiki/OODA_loop

LEARNING LESSONS

> *It's tough to make predictions, especially about the future.*

Yogi Berra

Nothing stands still and neither can preparations to ensure a firm's resilience. Events that happen to other firms should be studied carefully to see if lessons apply and changes are required to avoid a similar event occurring. Regulatory experts should involve not just other firms in financial services but right across the spectrum of relevant organizations (Did Travelex[8] absorb the lessons of the WannaCry ransomware attack on the NHS in May 2017[9]?).

The same goes for the outcome of events, real and simulated, that happen to a firm directly. There should be robust 'post-mortems' for service disruptions to ensure that all lessons are learned and that the resilience arrangements worked as intended. These should be documented to demonstrate reasonable steps taken in to supervision.

At the very least, this review should be part of the completion of the annual self-certification process. It should be no surprise that firms that have been more seriously impacted by events in the past are the ones who are more resilient going forward having seen the impact both on the bottom line and senior management.

WHAT NEXT?

The increasing complexity of the financial ecosystem and with it the greater risk of disruption warrants a greater focus on how to manage when the inevitable event happens. The key to firms successfully remaining within defined impact tolerances when there is a disruption is in the thoroughness of the preparations, realism in rehearsing the systems and the team involved in managing the response and the rigor with which lessons are applied. A self-critical approach where disruptions are expected, and an open culture focused more on addressing mistakes and issues than identifying who is to blame will also improve a firm's likelihood of being operationally resilient.

8. https://www.bbc.co.uk/news/business-51034731
9. https://www.bbc.co.uk/news/health-39899646

CONTACTS

Will Packard, Managing Principal
will.packard@capco.com

James Arnett, Partner
james.arnett@capco.com

Owen Jelf, Partner
owen.jelf@capco.com

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at www.capco.com, or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Hong Kong
Kuala Lumpur
Pune
Singapore

EUROPE
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO
THE FUTURE. NOW.