CAPCO

MANAGING THE INEVITABLE

A PRIMER ON OPERATIONAL RESILIENCE

TABLE OF CONTENTS

MANAGING THE INEVITABLE: A PRIMER ON OPERATIONAL RESILIENCE

In recent years 'expect the unexpected' has become something of a mantra for a great many of us. Yet, when viewed retrospectively, many of the events we have experienced or witnessed have come to possess a sense of inevitability – whether large scale cyberattacks, data outages, supplier process failures, disrupted commutes, terror incidents, extreme weather events or even pandemics. And while there is typically nothing that links these occurrences, they have all to varying degrees disrupted the ability of financial services firms globally to provide their customers with the expected level of service and support.

The financial ecosystem is becoming ever more complex due to greater outsourcing, wider adoption of cloud computing and the emergence of fintechs across more points within the value chain. All increase the potential for disruption to services; at the same time, firms must cope with enhanced expectations from customers and regulators alike.

Operational resilience is a critical factor to managing these pressures effectively. The underlying assumption behind operational resilience is that events will occur and that firms need to prepare accordingly. It is no longer a question of 'if' but 'when'.

Operational resilience is a broad regulatory theme rather than point regulation. The BCBS published a series of principles[1] on the topic in April 2021 and the UK's Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) are taking the lead publishing regulation earlier the same week. We expect other regulators to follow the UK lead if it is successful (and this is born out by a consultation paper[2] from the Central Bank of Ireland published in early April 2021 that follows the UK regulators' approach).

We view the UK regulators' approach as logical, coherent and provides a solid approach that will allow firms to improve their operational resilience. For this reason, it is worth reviewing the contents of their policy and supervisory statements in more detail.

The definition of operational resilience[3] 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 with no defined end state; as the threat evolves so should the responses of firms. The regulators are focusing on the approach that is taken and how seriously the topic is taken by firms management.

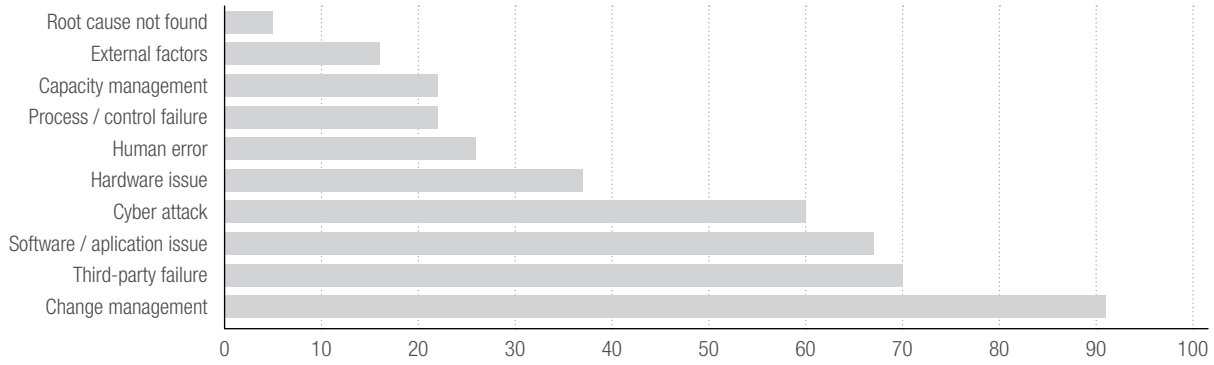
It is not operational risk; It is about managing the response to a situation that has already happened and not about the likelihood of an event and quantifying the resulting financial impact. It is focused on the broad impact on customers and financial stability rather than the more horizontal/internal focus of Business Continuity Planning (BCP) and Operational Continuity in Resolution (OCIR)/Recovery and Resolution Planning (RRP).

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 decision-making around service and product offerings. The analysis needs to be refreshed regularly and the response to potential events rehearsed on a frequent basis. It is for this reason that UK regulators are requiring annual sign off from legal entity boards on the operational resilience of their firms.

It would also be wrong to assume that operational resilience revolves primarily around cyber threats; most service disruptions are caused by internal errors such as the issues around the TSB data migration in 2018 following its sale from Lloyds to Sabadell[4]. The following chart shows the number of disruptions reported to the FCA in 2017 and 2018 by type.

1. https://www.bis.org/bcbs/publ/d509.htm
2. https://www.centralbank.ie/docs/default-source/publications/consultation-papers/cp140/cp140---cross-industry-guidance-on-operational-resilience.pdf?sfvrsn=5
3. https://publications.parliament.uk/pa/cm201919/cmselect/cmtreasy/224/224.pdf
4. 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)



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

In the UK 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 legal entity boards or branch management committees. 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 to take' The expectation is for firms to prioritise their services in terms of harm to their clients/customers and then set a defined maximum time of disruption is also a departure from the previous approach.

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; larger, more significant firms are expected to progress more rapidly.

With the PRA focused on financial stability and the soundness of firms and the FCA concerns centered on harm to clients the latter will typically result in a lower impact tolerance.

The regulation applies to:

PRA Scope: Systemically important institutions (O-SIIs), Solvency II firms, Insurers with gross written premiums exceeding £10 billion or technical provisions exceeding £75 billion, both on a 3-year rolling average. Smaller firms DO NOT have to assess their potential impact on financial stability when identifying Important Business Services and setting Impact Tolerances.

FCA Scope: enhanced scope SMCR firms, banks, designated investment firms, building societies, Solvency II firms, UK RIEs and electronic money institutions/payment institutions/registered account information service providers.

By 31 Mar 2022 (Implementation Deadline): Firms should have identified important Business Services, set impact tolerances, carried out mapping and scenario testing to a level which allows them to identify vulnerabilities. Firms also should have completed an initial self assessment.

By 31 Mar 2025 (Transition Deadline): Firms should have performed full mapping and testing and made investments to enable them to operate consistently within impact tolerances.

Operational resilience self-assessment to be available to regulators NO earlier than 31 Mar 2022. We anticipate that boards are going to want to have a good idea of vulnerabilities before signing off on the firm's resilience preparations so initial mapping and scenario testing will need to have identified gaps.

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 prioritising and 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 UK 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. The incident response apparatus should also be rehearsed regularly.

PREPARING FOR THE INEVITABLE

Identification of important Business Services

The starting point is identifying the important business services that 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, renewing an insurance policy and the suchlike. They are not internal systems such as a general ledger, HR database or business lines such as mortgages or foreign exchange. The prioritisation of Business Services and the identification of which ones are important should be based on harm to customers, impact to market stability and integrity and harm to the firm.

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, impact on market stability/ integrity and impact to the soundness of the firm. Impact tolerances should take into account relevant factors such as the number of customers affected and financial loss to them, data integrity, substitutability, time of day, etc.

Dual regulated firms will need to consider both the PRA and FCA priorities when setting impact tolerances that may lead to a separate value for each regulator. We expect firms typically to set just one impact tolerance for each IBS which the regulators acknowledge as acceptable provided thought has been given to the priorities of each.

PREPARING FOR THE INEVITABLE (CONTINUED)

Mapping

To be able to identify vulnerabilities and conduct scenario testing the processes that deliver Important Business Services first need to be mapped. Parameters such as the nature and time taken to implement the recovery solution 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 elements in a process that potentially could cause disruption. There is no need to include the mapping documentation in the annual self-certification.

Methodologies like Digital Twins can make this step not only a better representation of the reality on the ground but also easier to create as well as delivering greater utility in managing incidents and also process design.

The process maps need to include details on outsourced elements of the processes; we expect this to be one of the larger bodies of work that firms need to undertake to meet the UK regulation.

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 mandating 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 element of the process can be undertaken. Some of these will be more general than others (local power outtage 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 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

Firms need to test the resilience of the processes that deliver their IBSs for a series of severe but plausible events based on the information in the process mapping. The regulators have indicated that severe but plausible covers events that impacted organisations globally already. They have also indicated that scenario testing should be carried out regularly or if there are material changes to the service or the processes that deliver it.

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)

We anticipate that given the weight that boards will put on scenario testing and the number of possible scenarios that firms will want to test their IBSs at least annually on an ongoing basis. During the initial uplift to meet the regulations and to demonstrate that vulnerabilities have been remediated we expect firms to carry out considerably more testing. The example given in the consultation papers was four scenarios for a given Important Business Service. The regulators also indicate that some particularly severe scenarios that the firm is unlikely to pass should also be selected. This will help calibrate the level of resilience in a firm.

The FRBNY guidance published last October mentions that Scenario testing should be carried out semi-independently of the team responsible for the resilience of the IBS which we will give boards more confidence in the validity of the results.

Firms should also look to test the information on recovery method and time taken that is included in the process mapping. This should be practical testing to ensure that the stated solution works in the time stated.

Self-assessment

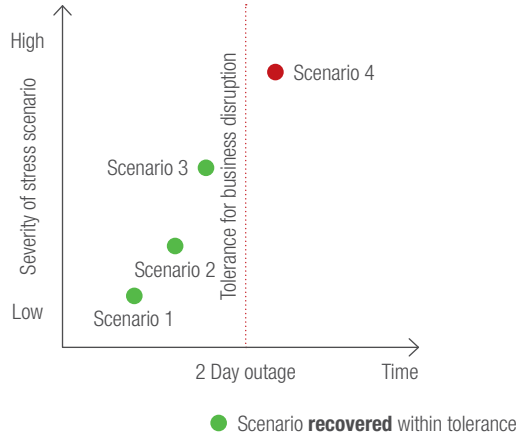
The relevant senior managers and the board should sign off that their firm can remain within its impact tolerances given disruption to its processes, detailing the important Business Services, the relevant impact tolerances, third-party dependencies as well as the results from the scenario testing. There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

Annual review

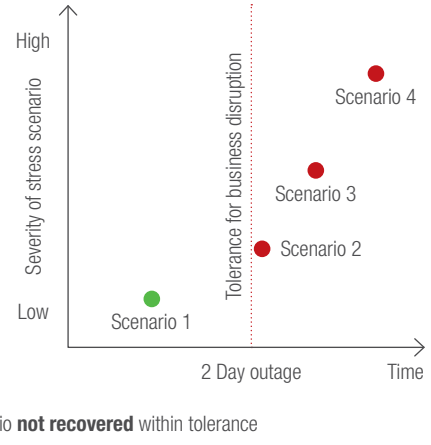
While changes to processes should be made as soon as the need is identified (e.g. due to an event that has happened at a competitor) all the steps covered already should be reviewed on at least an annual basis to identify any changes and drive remediation. One key element is using scenario testing to 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 managers and the board.

Examples of the results of scenario testing

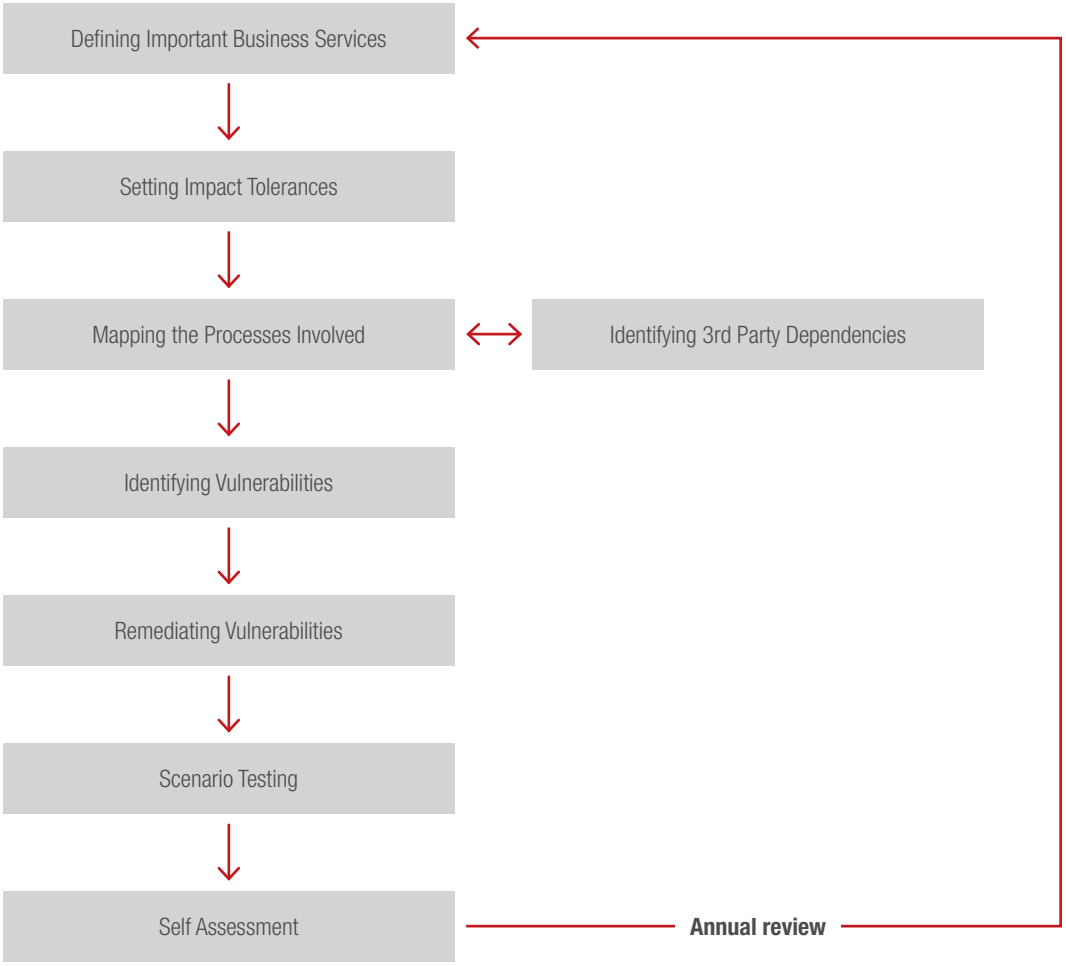
Case one: A firm considers its impact tolerance against severe but plausible scenarios. Here operational resilience is sufficient – it is disproportionate to expect the firm not to breach its impact tolerance in the extreme scenario of scenario 4.



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



The steps involved in operational resilience



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.

The need to remain within impact tolerances will lead to firms becoming much more proactive in addressing disruption with an emphasis on early warning and well practiced responses.

Identifying the right decision-making bodies 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.

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 status should be designed in from system inception and allow for rapid aggregation. Information on the status of a firm's processes should be readily available and visualized in a way that facilitates understanding. Best practice for example 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). 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 who are experienced in decision-making in fast moving situations to ensure that best practice is adopted. One approach used by 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 improved in terms of quality of decision making and timeliness and when recombined the loop is run at pace to gain and retain the initiative. This can be adapted to managing a response in an operational resilience context.

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

LEARNING THE 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.

This 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 supervision.

At the very least, this review should be part of the completion of the annual self-certification process. The harder a firm prepares and trains to manage events the better the outcome when the inevitable happens.

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 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
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

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

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

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO