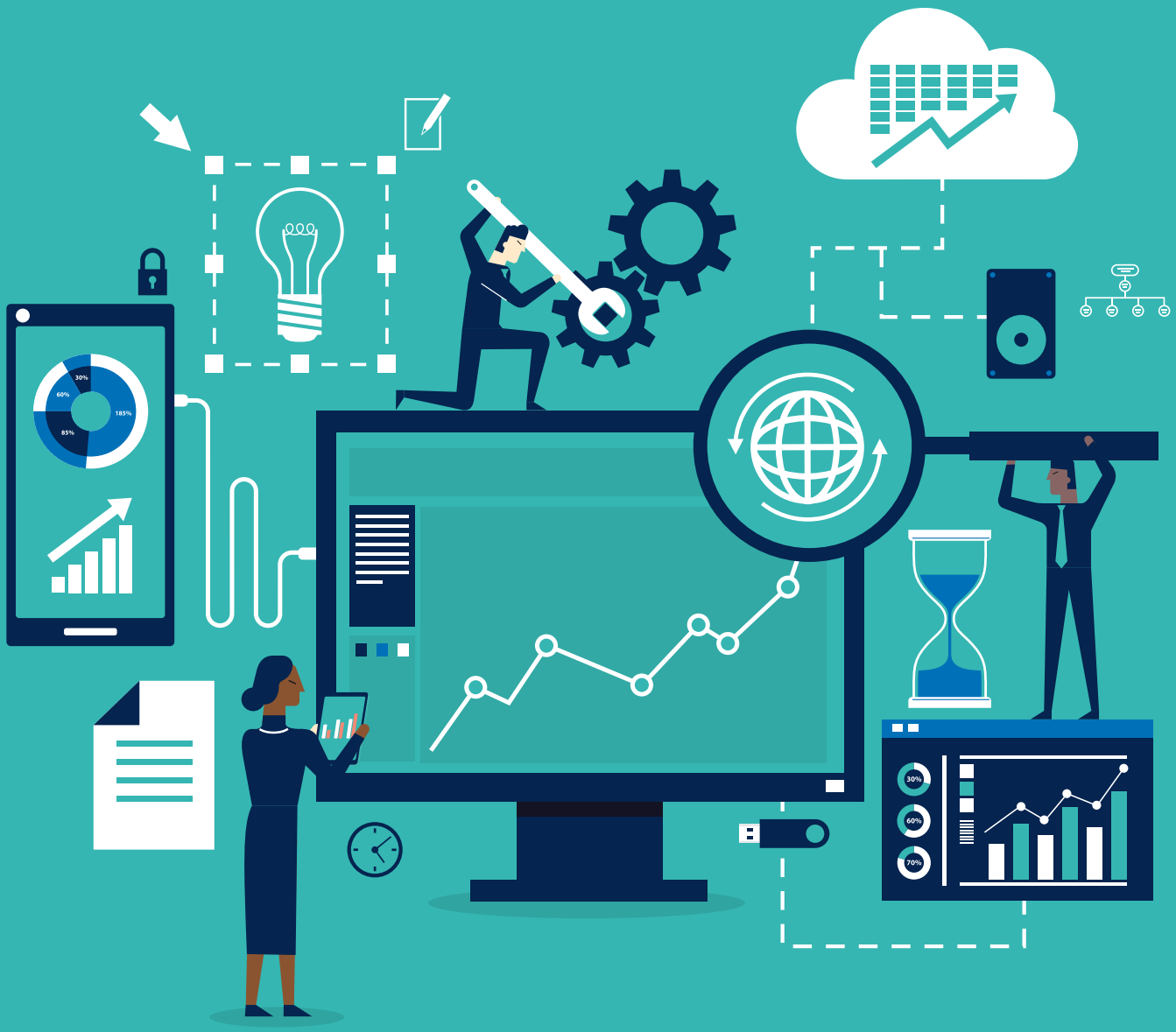
THE INVESTMENT ASSOCIATION

OPERATIONAL RESILIENCE:

SEVERE BUT PLAUSIBLE SCENARIOS

March 2024



ABOUT
THE INVESTMENT ASSOCIATION (IA):

The Investment Association champions UK investment management, supporting British savers, investors and businesses. Our 250 members manage £8.8 trillion of assets and the investment management industry supports 126,400 jobs across the UK.

Our mission is to make investment better. Better for clients, so they achieve their financial goals. Better for companies, so they get the capital they need to grow. And better for the economy, so everyone prospers.

Our purpose is to ensure investment managers are in the best possible position to:

- Build people's resilience to financial adversity
- Help people achieve their financial aspirations
- Enable people to maintain a decent standard of living as they grow older
- Contribute to economic growth through the efficient allocation of capital.

The money our members manage is in a wide variety of investment vehicles including authorised investment funds, pension funds and stocks and shares ISAs.

The UK is the second largest investment management centre in the world, after the US and manages 37% of all assets managed in Europe.

CONTENTS

1. INTRODUCTION

When issuing the operational resilience policy, the regulatory authorities understood that firms, as well as themselves, would learn during the implementation period. The regulators also envisioned that best practice would emerge over time, and they indicated that they would take a close interest as it develops. The concept of severe but plausible is one such area where building a common understanding and sharing best practice will be beneficial. This document represents the IA's contribution in this regard.

In late July 2023, the IA convened the Severe but Plausible Working Group (the Working Group) to explore this area in detail. The group, made up of 14 member firms and supported by PwC, met a total of 5 times to discuss the subject and produce a library of baseline severe but plausible (SBP) scenarios that readers may use as a starting point for calibrating severe but plausible scenarios for their own firm.

We would like to thank PwC for providing their support and expertise and members of the Working Group for sharing their insights over the course of this project.

The Working Group and this document set out to:

- Address some of the ambiguity surrounding the SBP concept, helping to make the operational resilience policy clearer to understand in this area, and potentially, lead to more effective implementation.
- Identify best practices in calibrating SBP scenarios.
- Provide baseline information that firms can use as a starting point to calibrate SBP scenarios appropriate for their own businesses, accompanied by supporting guidance and considerations to be thought through (see Section 6: Severe but plausible scenario library).
- Build a common understanding of the factors and circumstances which are unlikely to be severe enough for effective testing.

HOW TO USE THIS GUIDE

This document builds directly on the IA's previous ***member guidance on Scenario Testing***, produced in December 2021. This previous guide focuses on how firms can approach their operational resilience scenario testing programme.

The Cross Market Operational Resilience Group (CMORG) has produced ***guidance*** on firm operational resilience, updated in November 2023. Section 5 of this guidance relates to scenario testing, including discussion on severity and plausibility. Readers are encouraged to examine the CMORG guidance alongside the contents of this document. This IA document is not intended to compete with or contradict the guidance contained with the CMORG paper, and it should be seen as a complementary resource for investment management firms.

For more detail on our previous work on Important Business Services, Operational Resilience Governance, Impact Tolerances, Self-Assessments and Third Party Risk Management, please refer to our dedicated expert page ***www.theia.org/operational-resilience***

2. CHALLENGES

The UK operational resilience policy is designed as an outcomes based policy. The emphasis is therefore relatively lighter on the policy detail, and the regulatory authorities consciously decided to not provide specific definitions or guidance for the foundational concepts of the policy such as SBP scenarios.

The benefit of this approach may be a more flexible and responsive policy over time. Severe but plausible is not a static concept. What constitutes SBP today may change over time as the risks facing firms and the market evolve. The approach also enables regulators to maintain an emphasis on resilience outcomes.

However, the trade-offs of this approach are greater ambiguity for firms having to implement the policy, and from the regulators' perspective, less consistent implementation across firms. Indeed, the IA has conducted benchmarking exercises with its members which revealed that there is uncertainty and differing interpretations across firms on what constitutes a SBP scenario.

In addition, the SBP concept embodies characteristics that add to the challenge for firms:

- Severe but plausible is idiosyncratic to individual firms. The regulators have stated 'the nature and severity of scenarios it is appropriate for firms to use may vary according to their size and complexity' (Operational Resilience: Impact tolerances for important business services, March 2021, page 10). This suggests that a proportionate level of severity for a smaller firm might not necessarily be severe enough for a larger one. It also implies that SBP scenarios are unlikely to be 'one size fits all'.

- The absence of a detailed definition leaves it to firms to form their own interpretation of what SBP means.

- Identifying SBP scenarios is not an entirely analytical or objective process. There is always an element of subjective professional judgement involved.

- Proportionality is integral to the concept, but it is unclear how to gauge it. Firms are not expected to be able to remain within impact tolerances in scenarios that are too severe or are implausible.

[1] https://www.handbook.fca.org.uk/handbook/glossary/G3505i.html?date=2022-03-31

3. REGULATORY REQUIREMENTS

Below is a summary of key points from various applicable regulatory sources which refer to the concept of SBP.

Senior Management Arrangements, Systems and Controls sourcebook (SYSC) – Specific rules:

- *15A.2.9 – R - A firm must ensure it can remain within its impact tolerance for each important business service in the event of a severe but plausible disruption to its operations.*
- *15A.5.3 – R - A firm must carry out scenario testing, to assess its ability to remain within its impact tolerance for each of its important business services in the event of a severe but plausible disruption of its operations.*

The FCA stipulates 5 scenarios firms should consider when conducting scenario testing:

1. corruption, deletion or manipulation of data critical to the delivery of important business services
2. unavailability of facilities or key people
3. unavailability of third-party services which are critical to the delivery of important business services
4. disruption to other market participants
5. loss or reduced provision of technology underpinning the delivery of important business services

FCA PS21/3, March 2021

- The FCA expects firms, by the end of the implementation period at the end of March 2025, to manage their business to ensure they can operate within impact tolerances at all times, including during **severe but plausible** scenarios. (page 17)
- Firms are expected to **test** their impact tolerances in a range of severe but plausible scenarios. (Page 19)
- The FCA envisions that where firms test in a variety of severe but plausible scenarios, it will enable firms to also effectively translate that effort in the event of an **unpredictable disruption**. Therefore, the purpose of the severe but plausible concept is as a planning tool for firms to ensure they are better equipped to remain within impact tolerances, both for severe but plausible scenarios, and for other unpredictable ones. (Page 19)
- Testing a range of severe but plausible scenarios is also intended to help firms **identify** areas where further resilience needs to be built. (Page34)

FCA CP19/32, December 2019

- In carrying out the scenario testing, firms should identify an appropriate range of adverse circumstances varying in nature, severity and duration **relevant to its business and risk profile**. (Page 22)
- The FCA considers that firms are best placed to determine the scenarios used for testing. When setting scenarios, firms could consider previous incidents or near misses within their organisation, across the financial sector and in other sectors and jurisdictions. Firms could also consider horizon risks, such as the evolving cyber threat, technological developments and business model changes. (Page 22)
- To cover a range of severe but plausible scenarios, firms could use an incremental process. For example, firms could:
- start by assuming disruption to the resources key to the delivery of important business services (the cause not being material)
- increase severity by assuming simultaneous disruptions to key resources of their important business services or by resources being unavailable for longer time periods. (Page 23)

PRA & FCA – *Operational Resilience: Impact tolerances for Important Business Services*, March 2021

- *5.11. To allow flexibility for firms and FMIs in their approach to operational resilience, the final policy expects that firms and FMIs identify the severe/extreme but plausible scenarios they use for testing. When setting severe/extreme but plausible scenarios, firms and FMIs could consider previous incidents or near misses within the organisation, across the financial sector and in other sectors and jurisdictions. A testing plan should include realistic assumptions and evolve as the firm learns from previous testing.*
- *5.12. The supervisory authorities see this area as one where the interest of firms and FMIs and the supervisory authorities should be aligned – if a firm or FMI chooses scenarios that are insufficiently severe/extreme, boards and senior management might be taking inappropriate risks with the running of their businesses.* ***The nature and severity of scenarios it is appropriate for firms to use may vary according to their size and complexity****. As a result, the policy does not include detailed guidance. However, the supervisory authorities anticipate that this will be a common area for supervisory discussion, including developing an understanding of how and why scenarios have been selected. The supervisory authorities expect best practice to develop over time and that both firms and FMIs, and the supervisory authorities will learn more over time.*

***PRA SS1/21*,** March 2022 (updating the March 2021 version)

- *6.10. The PRA recognises that it would not be proportionate to require [PRA regulated] firms to be able to remain within impact tolerances in circumstances which are beyond severe or implausible. There will be scenarios where firms find they could not deliver a particular important business service within their impact tolerance. For example, if essential infrastructure (such as power, transport, or telecommunications) were unavailable, some firms may not be able to deliver their important business services within their impact tolerance.*
- *6.12. Firms should test a range of scenarios, including those in which they anticipate exceeding their impact tolerance. Understanding the circumstances where it is impossible to stay within an impact tolerance will provide useful information to firms' management and to their supervisors. Boards and senior management will need to judge whether failing to remain within the impact tolerance in specific scenarios is acceptable and be able to explain their reasoning to supervisors.*
- *7.1. Boards must regularly review assessments of the firm's important business services, impact tolerances, and the scenario analyses of its ability to remain within the impact tolerance for these important business services.*
- *8.3. When documenting a self-assessment to meet the Operational Resilience Parts, firms should:*
  - *describe their strategy for testing their ability to deliver important business services within impact tolerances through severe but plausible scenarios. Firms should also describe the scenarios used, the types of testing undertaken, and specify the scenarios under which firms could not remain within their impact tolerances.*

FCA supervisory feedback that has been shared publicly:

- FCA has seen some examples of SBP scenarios that are not severe enough.
- SBP scenarios should be sufficiently stretching and should have the potential to push the firm beyond its impact tolerances.
- Firms should not rely exclusively on existing component testing (i.e., DR, ITSCM, BCM), and need to test their ability to maintain delivery of the important business service outcome to customers.

4. WORKING GROUP FINDINGS AND INSIGHTS

Through its discussions, the Working Group formed several findings, conclusions and illuminating insights that readers may benefit from reflecting on. The most important of these are summarised below.

4.1 'EXTREME BUT PLAUSIBLE' DOES NOT MEAN GREATER SEVERITY THAN 'SEVERE BUT PLAUSIBLE'

The Working Group found that there is significant confusion surrounding the distinction between SBP scenarios and extreme but plausible (EBP) scenarios.

A common misconception is that EBP scenarios are a more severe category of scenarios, above SBP, that are applicable to Financial Market Infrastructures (FMIs). However, this is not the case.

Through its discussions, the Working Group found that there is in fact no distinction between SBP and EBP scenarios, and the simultaneous use of the two terms has a technical explanation. In the BoE policy, the term extreme but plausible was adopted for FMIs because the definitions were derived from European legislation (such as CSDR), which uses the term extreme, and therefore the decision was taken to mirror that terminology for FMIs.

EBP does not mean a higher level of severity than SBP. For instance, it would not be appropriate to hold FMIs to a higher standard than certain non-FMIs such as global banks.

However, the confusion around SBP and EBP is mainly a terminology issue, as the policy does still envision proportionality. More complex, larger or systemically important firms will attract higher resilience expectations than less complex, smaller or not systemically important ones.

4.2 SBP SCENARIOS SHOULD CONSIDER A RANGE OF INCIDENT TYPES

The Working Group heard that SBP should include 'rapid onset' incidents that cannot be foreseen or have not been previously planned for, alongside incidents that could be the result of 'slow burn' disruption. For example, Covid-19 was a slow burn incident that, from the perspective of UK firms, could be seen coming several months out and could be planned for, in theory. However, firms still experienced disruption related to Covid-19 which impacted their ability to deliver IBS (e.g., disruption to offshore third party services). Therefore, SBP scenarios should include incidents that are both slow burn and onset quickly.

4.3 PLAUSIBILITY AND PROBABILITY

The plausibility of a scenario should not be conflated with its probability. A scenario can be plausible, even if its probability of occurring is low.

The Working Group heard that the operational resilience policy intends to shift firm thinking away from probability of an incident occurring and towards the plausibility of it occurring. This is because there are many improbable events that have none the less crystalised in the real world.

Some Working Group members stated they had developed internal definitions around plausibility to help guide scenario development.

4.4 STRETCH OR COMPLY?

The intention of the operational resilience policy is to generate deeper insights and a better understanding of the business and its resilience, which in turn will improve the firm's overall ability to respond to disruption. However, the Working Group found a tension between:

a. the requirement for firms to be able to remain within impact tolerances in the event of a SBP disruption to its operations by the end of the implementation period in March 2025 (i.e., to be compliant with the letter of the policy); and

b. the expectation of regulators to escalate the severity of their scenario testing to understand the point at which they may no longer be able to maintain the service within tolerance, and so demonstrate the limits of a firm's ability and the choices and/or prioritisation they need to make to improve their resiliency (i.e., to stretch SBP scenarios).

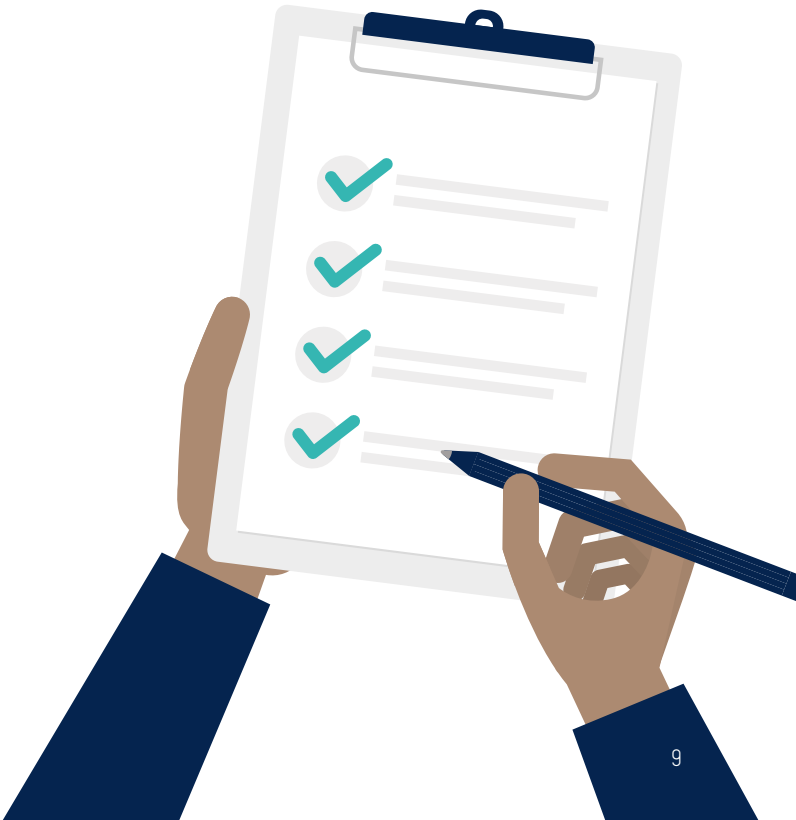
Working Group members were concerned that if their SBP scenarios were expected to be continually developed and stretched with reference to their ability to challenge impact tolerances during testing, this could result in the development of disproportionately severe scenarios.

On the other hand, where a firm opts to take a compliance-led approach to testing, the downside could be a testing programme that does little to improve understanding of the firm's resilience, and consequently, does not build a robust set of evidence with which to assuage regulatory supervisors. Potentially, regulatory supervisors may be sceptical towards seemingly compliant firms who have not identified weaknesses or areas for improvement.

The Working Group concludes that this is an area that would benefit from further clarification from the regulatory authorities. It ought to be possible for firms to both demonstrate their compliance with the policy and to confidently push the boundaries in their testing when and where appropriate. We have suggested some strategies firms may wish to adopt in this regard in section 6.3 of this paper.

4.5 ROOT CAUSES ARE LESS IMPORTANT THAN THE IMPACT ON IMPORTANT BUSINESS SERVICES

Scenario tests contribute to the portfolio of evidence, against specific disruption scenarios, which is gathered over a period of time and from multiple sources, similar to financial stress testing. Each point in time test(s) should inform but should not exclusively define a firm's resilience capability, or the remediation needed to enhance it. Including a root-cause to the disruption within the test increases plausibility on the impact from disruption and could support the response required from firms to deliver their IBS within impact tolerance. For example, if the root cause of the unavailability of the investment management team is sickness, the firm should consider which other teams might be at risk of suffering from illness and how this informs a firm's response.



4.6 THE DEVELOPMENT OF CYBER SCENARIOS REQUIRES ADDITIONAL CONSIDERATIONS

The Working Group discussed whether cyber incidents should be thought of as a distinct category of scenarios or should simply be considered a root cause of various other technology scenarios.

Ultimately, it was concluded that cyber scenarios should be developed with additional considerations, including a longer duration of impact, compared to other technology scenarios. These scenarios are also distinct from other types of scenarios in their deliberate intent to cause harm and how they go beyond the technical aspects of recovery such as the impact on and reliability of alternative systems or back-ups in a cyberattack scenario.

Within the cyber category, ransomware scenarios should feature in firms' planning as this is a high priority area for regulators. Firms should consider how they would respond to different types of ransomware scenarios, including destructive ransomware (also known as wiper malware) and ransomware incidents in the supply chain.

It was acknowledged that cyber resilience is likely to be an area where many firms will have further work to do, even beyond the final implementation deadline in March 2025. This is owing to the magnitude of the risk, the ever-evolving tactics of malicious actors and the inherent difficulty and expense of achieving robust cyber resilience. Numerous real-world examples of effective cyber-attacks, including against state institutions, demonstrate that organisations of all types are likely to remain vulnerable to cyber-attacks to some extent, at least for the foreseeable future.

4.7 THIRD PARTY SCENARIOS ALSO REQUIRE ADDITIONAL CONSIDERATIONS

The Working Group highlighted that third party scenarios also require additional considerations. Disruption to key third party providers, such as the loss of a custodian or a core trading platform, has the potential to result in exceeding impact tolerances because of the complexity of moving to an alternative provider, the volume of transactions and the time involved in setting up accounts in another system.

4.8 DATA LOSS / THEFT

The Working Group discussed data loss scenarios stemming from data theft. There are many serious issues as a result from data loss, such as potential harm to customers and staff, reputational damage, and in the case of personal data, serious regulatory breaches. However, the loss of data/ confidentiality was not necessarily considered an operational resilience incident in the strictest sense because the firm's operations and IBSs are not directly disrupted.

That is not to say, however, that data loss cannot translate into operational disruption. It can. Data loss will factor into different aspects of recovery and how an incident is managed. Data theft also raises questions over data integrity and can lead to firms locking down systems to prevent further data theft, which in turn can interrupt IBSs.

In conclusion, data theft is best thought of as a root cause of other types of disruption.

5. HOW TO APPROACH SEVERE BUT PLAUSIBLE SCENARIOS

Readers are reminded at this point that this guide builds on the IA's previous ***member guidance on Scenario Testing***, produced in December 2021.

The Working Group identified general considerations for approaching SBP scenario calibration. These included:

- At the outset, remember the purpose of testing. Testing of severe but plausible scenarios is a planning tool for helping firms better understand the level of disruption they can withstand, and what they cannot.
- Firms can focus on testing known areas of weakness (more plausible) and exploring new areas (less plausible but potentially more informative).
- Firms should consider compound scenarios, where multiple incidents occur simultaneously, as a means of increasing severity.
- Duration can often be the key driver of severity. Duration also is a large factor in determining the plausibility of a given scenario.
- The level of severity a firm concludes is appropriate to calibrate their SBP scenarios is not necessarily the level of severity that the firm will run their tests at. This is because firms may choose to ramp up the level of severity even further during testing to gather more insights and understand the point at which tolerances are exceeded. See '**4.4 Stretch or comply?**' and '**6.3 Additional considerations**' for further discussion on this point.
- Firms should also consider scenarios that could have a wider impact on other firms, especially as it relates to maintaining or undermining confidence in the firm or the wider financial system, or potentially triggering a disorderly market.
- Documenting the rationale as to why a particular resource/ resources have been selected for the scenario and how it has been calibrated is key, including what lessons the firm hopes to learn from the test and the potential to find unknown risks/ vulnerabilities for the firm in the process.
- Firms should compile a scenario library covering a range of adverse circumstances of varying nature, severity and duration relevant to its business and risk profile and consider the risks to the delivery of the firm's IBS in those circumstances. The results of testing need to be reported to and understood at the board level.

6. SEVERE BUT PLAUSIBLE SCENARIO LIBRARY

The aim of the 'severe but plausible scenario library' is to collate the views and experience from Working Group members to provide firms with additional guidelines on developing their own test scenarios. The library is meant to be a reference point for firms to calibrate their testing against, but it is not expected that firms use these scenarios exactly as described. Rather, firms should use this library as a basis to challenge their own thinking and augment their existing approach to scenario testing. Furthermore, this library is not intended to be an exhaustive list of possible scenarios, and firms should seek to develop their own libraries considering their own environment and reflecting the risks specific to their own businesses.

The library was developed through the analysis of the scenarios used by Working Group members in their own operational resilience scenario testing exercises. It was further supported by research and evaluation of "real life" disruption incidents experienced by other investment management firms, wider financial services firms, and large companies across a range of industries. This helped ensure the scenarios were evidence based, and could be justified as being both realistically severe and also entirely plausible.

6.1 SEVERE BUT PLAUSIBLE SCENARIO LIBRARY

Pillar	Scenario Impact	Duration (short)	Duration (long)	Scenario Potential Root Cause (source: Working Group members)
People	Unavailability of 20% of FTEs from all teams that supports delivery of an important business service.	2 weeks	1 month	- Staff shortage to support service delivery due to illness during a pandemic - Outbreak of illness (e.g. Legionnaires' disease) causing location-specific colleague unavailability - Geopolitical events, such as conflicts or government actions, causing migration or limiting workforce mobility - Union strike impacting restricting individuals' willingness to work
People	Loss of the head of a team that supports delivery of an important business service.	1 month	3 months	- Sudden departure of key personnel due to unforeseen circumstances such as illness, accidents, or personal emergencies
Facilities	Total unavailability of a facility (e.g. office) that supports delivery of an important business service.	24 hours	6 months	- Local infrastructure failures (e.g. power outages, HVAC malfunction) including backup capabilities - Loss of critical national infrastructure (e.g. power, water) - Natural disasters (e.g. earthquakes, floods, fires) - Man-made disasters (e.g. crime, civil unrest, terrorism, war)
Facilities	Total unavailability of a facility (e.g. data centre) that supports delivery of an important business service.	24 hours	6 months	- Local infrastructure failures (e.g. power outages, HVAC malfunction) including backup capabilities - Loss of critical national infrastructure (e.g. power, water) - Natural disasters (e.g. earthquakes, floods, fires) - Man-made disasters (e.g. crime, civil unrest, terrorism, war)
Facilities	Cyberattack on a facility (e.g. core data centre infrastructure) that supports delivery of an important business service.	72 hours	2 weeks	- Cyberattacks like Distributed Denial of Service (DDoS), malware and ransomware affecting IT infrastructure
Technology	Complete loss of a single technology that underpins the delivery of an important business service.	48 hours	120 hours	- Software bugs in the order management system - Aging software without upgrades - Application failure due to insufficient testing and validation following upgrade - Software bugs causing application crashes and instability - Failed implementation of a change to a critical application, resulting in system unavailability and business process disruptions.
Technology	Complete loss of more than one technology that underpin the delivery of an important business service.	24 hours	72 hours	- Aging hardware without upgrades and maintenance - Improper infrastructure change configuration leading to system issues - Hardware failures, including servers, network devices, and storage systems - Disruption or loss of core infrastructure services due to malware or other causes like device or OS related compromise and failed changes. - Full network/core infrastructure outage - Outage of the primary data centre

Pillar	Scenario Impact	Duration (short)	Duration (long)	Scenario Potential Root Cause (source: Working Group members)
Technology	Ransomware attack affecting one or more technologies that support the delivery of an important business service	72 hours	2 weeks	- Insider threats and inadequate information security - Cyberattacks like DDoS and ransomware affecting key technology systems
Technology	Destructive ransomware attack affecting one or more technologies that support the delivery of an important business service	72 hours	2 weeks	- Destructive ransomware (also known as wiper malware) that destroys affected data or incapacitates affected systems or devices, even if any accompanying ransom demands are paid - Destructive ransomware is often associated with malicious state-backed actors, but can also be deployed by criminal groups
Data	Corruption of a significant proportion of the data critical to the delivery of an important business service.	24 hours	48 hours	- Hardware or software failures in critical systems, resulting in the inability to access and process data. - Errors during data handling or processing, resulting in inaccurate information.
Data	Deletion or loss to access to a significant proportion of the data critical to the delivery of an important business service.	24 hours	48 hours	- Human error during data entry without proper verification, leading to critical data source overwriting and application failure. - Critical data source being overwritten due to inadequate training and process controls. - Mistake by staff in charge of data entry, overwriting critical data source. - Technical issues like data storage failures or database corruption leading to data unavailability.
Data	Cyberattack leads to breach of data critical to the delivery of an important business service.	72 hours	2 weeks	- Ransomware attack leading to data loss and system rebuild. Loss of sensitive data, operational disruption, and costly efforts to restore systems and data - Insider threat from and inadequate data security. - Insufficient cybersecurity measures i.e. malicious phishing emails - Insider threats or unauthorised access to data. - Types of Communication Attacks that illicit actors use are, but are not limited to: DNS Hijacking, Man-in-the-middle attacks, Zoom-bombing
Third Parties	Unavailability of a single systemic technology provider critical to the delivery of an important business service.	12 hours	24 hours	- Geopolitical events impacting supplier operations disrupt services provided to the firm - Outage of a major cloud service provider's primary data centre campus - Outage of a major cloud service provider's primary data centre region - Data integration issues between internal systems and external third-party platforms - Vendor mismanagement or financial instability leading to service disruptions
Third Parties	Unavailability of a single non-systemic technology provider critical to the delivery of an important business service.	24 hours	48 hours	- Lack of redundancy and failover mechanisms with technology providers - Denial of access to a critical technology supplier's core location due to unforeseen circumstances, disrupting their services provided to the firm
Third Parties	Unavailability of a single systemic outsourced service provider critical to the delivery of an important business service.	24 hours	48 hours	- Infrastructure failure with critical supplier, impacting its ability to provide services
Third Parties	Unavailability of a single non-systemic outsourced service provider critical to the delivery of an important business service.	48 hours	72 hours	- Issues arising from new outsourcing arrangements disrupt operational stability - Communication breakdowns with third-party service providers - Inadequate performance monitoring and service level agreements
Third Parties	Outage of a single FMI critical to the delivery of an important business service.	2 hours	24 hours	- Outage of financial market infrastructure (e.g. SWIFT, LSE, LCH, Euroclear) - Disruption to the asset manager's connection to the FMI to be considered under 'Technology' scenarios
Third Parties	Cyber attack at a third party vendor supporting an important business service	24 hours	2 weeks	- Cyberattack on a critical supplier's systems, affecting a firm's services as they rely on the supplier for essential operations - Denial of access to a critical supplier's core location due to unforeseen circumstances, disrupting their services provided to the firm - Cyberattacks targeting third-party systems and infrastructure

6.2 HOW TO USE THE LIBRARY

The scenario test library is primarily designed with mitigating harm to consumers in mind. In general, inflicting harm on consumers is likely to be the biggest concern for the investment management industry rather than causing a risk to market integrity or broader financial stability. However, the scenarios may still be appropriate for dual-regulated insurers testing their policyholder protection impact tolerances, if deemed applicable.

Firms required to set additional impact tolerances for the point at which further disruption to an IBS would pose a risk to the firm's safety and soundness or market integrity may need to consider scenarios with longer durations to test these.

The scenario test library has been structured by resource pillar (people, facilities, technology, data, and third parties), with suggested 'impact scenarios' provided for each pillar. As mentioned above, Working Group members were of the view that testing a firm's ability to recover from a specific impact was a preferable starting point (and better aligned to regulatory expectations) than testing a firm's ability to recover from a specific root cause, which may or may not have a significant impact on the IBS.

Under this 'impact scenario' approach, resources are effectively assumed to be completely or partially unavailable for a duration of time. The library provides suggested 'short' and 'long' durations for each scenario recognising the different types of impacts. These suggested durations are intended to be used as 'guide rails' for what the Working Group considered severe but plausible (i.e. durations less than 'short' may not be sufficiently severe; durations longer than 'long' may start to stretch plausibility), but individual firms may choose to develop scenarios appropriate to them that consider durations outside of these ranges. It was acknowledged that calibrating SBP scenarios around the duration of a resource being unavailable was different to calibrating a SBP root cause (i.e. the risks / threats faced by a firm), and that in reality firms may wish to use a combination of the two.

To this end, potential 'root causes' of each scenario impact were also included, again based on Working Group members' experiences. Including a root cause within the scenario helps to increase the plausibility and realism of the testing. It can also be a key factor that drives the response a firm would take and how it would recover its service within impact tolerance effectively.

As noted in Section 4.6 above, separate cyber scenarios have been included within the library. These scenarios have suggested impact durations reflecting the unique nature of these incidents, and it will be up to individual firms to determine if these are suitable for their business.

Whilst the library can be read as a collection of single scenarios across each line, when developing their own scenarios, firms are encouraged to take elements from across the library (i.e. resource impacts, durations and root causes) to develop detailed scenarios suitable to their own firm. Firms are also encouraged to consider combining scenarios from across pillars as they seek to build the sophistication of their testing by impacting multiple resources and/or multiple IBSs.

6.3 ADDITIONAL CONSIDERATIONS

As discussed earlier in this paper, there is a potential conflict between developing scenarios that a firm considers SBP, and then also 'testing to failure', which might require a scenario that goes beyond the firm's definition of SBP.

A suggested approach put forward by the Working Group is for firms to develop their baseline SBP scenario, and then also include one or more 'stress factors' to layer into the scenario during testing. These stress factors would increase the severity of the scenario and would be included during the test to help firms understand when the scenario might become too severe for the service to remain within impact tolerance.

We understand that regulators have responded positively to firms that have presented scenarios where they do not believe they can remain within impact tolerance, whether this is because the firm has vulnerabilities that need to be addressed, or because the scenario is considered to be beyond SBP.

When exploring scenarios that go beyond SBP, either through testing or thought exercises, the key questions for firms to ask themselves are:

- what does the firm's resilience look like in this scenario?
- are there any reasonable actions that would limit the period of disruption?

In this way, scenarios that are beyond what is proportional for firms to recover from within impact tolerances may still be usefully considered to build on the firm's understanding of its resilience posture and identify if there are any viable actions that may be taken to improve the firm's resilience.

The Investment Association
Camomile Court, 23 Camomile Street, London, EC3A 7LL

www.theia.org
@InvAssoc

March 2024