THE INVESTMENT ASSOCIATION

SCENARIO TESTING:

Severe but Plausible

December 2021

ABOUT THE INVESTMENT ASSOCIATION (IA):

The IA champions UK investment management, supporting British savers, investors and businesses. Our 270 members manage £9.4 trillion of assets and the investment management industry supports 114,000 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. FOREWORD

"TESTING IN A RANGE OF SEVERE BUT PLAUSIBLE SCENARIOS IS INTENDED TO HELP FIRMS IDENTIFY AREAS WHERE FURTHER RESILIENCE NEEDS TO BE BUILT. IN CARRYING OUT TESTING AND REMEDIATING ANY VULNERABILITIES, FIRMS SHOULD IN TURN BE BETTER PREPARED FOR POTENTIAL REAL-LIFE DISRUPTION AND REDUCE THE NUMBER OF SUCH DISRUPTIONS WHICH COULD CAUSE INTOLERABLE HARM TO CONSUMERS AND/OR RISK TO MARKET INTEGRITY." – **FCA, PS21/3.**

The Financial Conduct Authority (FCA) make it abundantly clear that testing a firm's ability to remain within its impact tolerances set for each important business service in severe but plausible scenarios is crucial to building and improving a firm's operational resilience. The regulator also stresses that firms should be making progress with their scenario testing as soon as is reasonably practical rather than waiting until the end of the transitional arrangements period. This paper addresses the regulators' expectations in this area and offers a series of considerations members can take forward and apply to their own firms in a proportionate manner when creating and conducting scenario tests. Scenario testing should be considered a preventative measure to enable firms to be better prepared when disruption occurs to minimise harm to consumers and market integrity.

Representing the fifth in our operational resilience series, this paper is intended to help members operationalise the different aspects of the FCA's rules. Given that the majority of our members are single, rather than dual-regulated, we have predominantly focussed on addressing the FCA's scenario testing requirements, although we do consider some aspects of the Prudential Regulation Authority (PRA)'s rules in this area too.

We emphasise throughout, the importance of building your operational resilience maturity over time. The regulators emphasise that they do not need to see a complete testing picture by March 2022 but rather want to see how firms will be developing their sophistication in this area. Whether at the start or at a more advanced stage, this paper offers considerations for all members. Members are invited to apply the considerations outlined and tailor them to reflect their individual circumstances and business model. For more detail on our previous work on Important Business Services, Operational Resilience Governance and Impact Tolerances, please refer to our dedicated expert page **www.theia.org/operational-resilience**

We would also like to thank KPMG for helping us with the Scenario Testing Working Group and sharing their insights and expertise.

Pauline Hawkes-Bunyan
Director, Business: Risk, Culture & Resilience
at The Investment Association

2. INTRODUCTION

The IA Scenario Testing Working Group (Working Group), set up in conjunction with KPMG, was launched in May 2021 to address the regulatory requirement for enhanced firms under SM&CR to conduct scenario testing for a range of severe but plausible scenarios. The group, made up of just under 20 member firms from a range of sizes and business models, met intensively over the summer and into the autumn of 2021. This paper represents the final output of this Working Group and has been informed by the discussions held.

WHAT IS SCENARIO TESTING AND WHY IS IT IMPORTANT?

Scenario testing enables firms to gain a comprehensive understanding of the resilience of their important business services and identify areas where action needs to be taken to remediate vulnerabilities to build their resilience over time.

Testing is also crucial to assess a firm's impact tolerances and determine whether the firm's incident response/playbook is fit for purpose to ensure the firm can recover the service within the tolerance defined. Understanding the severe but plausible scenarios where a firm is unable to remain within the impact tolerances it has set is just as important as understanding the instances in which a firm can meet their tolerances. The Board may also need to be engaged to determine whether additional investment is needed to address findings from scenarios where firms would breach their impact tolerances.

Please note that where we refer to 'scenario testing', this also incorporates scenario exercises.

HOW DOES SCENARIO TESTING DIFFER FROM EXISTING APPROACHES TO TESTING?

Existing testing strategies can be leveraged to inform approaches to scenario testing. However, in many ways scenario testing differs from business continuity, disaster recovery or financial stress testing. An end-to-end service resilience lens needs to be applied and a shift in focus to determine where the point of intolerable harm is reached in severe but plausible scenarios. Previously, some testing was centred around mitigating harm to the firm and the wider market. Now, the regulators are explicitly requiring firms to think about preventing intolerable harm manifesting to consumers too. Firms should also consider that harm may manifest in different ways for institutional and retail consumers.

Overview of document

This paper begins by offering a consideration of the necessary pre-requisites firms should have in place before looking to conduct scenario testing. The document then looks in more detail at the regulatory requirements in **Section 3** as well as providing an overview of the international regulatory landscape. **Section 4** covers what the FCA requires firms to detail in their scenario testing plans. Building on this, **Section 5** focuses on designing service-specific scenario tests, offering considerations on how firms can build scenario libraries.

Firms have a number of scenario options ranging from desktop workshops to live testing, and these are explored in more detail in **Section 6**. This paper also provides an overview in **Section 7** of approaches to collating data to inform scenario tests, as well as insights into the common challenge of gathering consumer harm data.

Many firms use third parties for the provision of all, or part of, their important business service. The regulators require firms to take certain third party risk management (TPRM) measures. **Section 8** looks at the regulatory requirements and provides suggestions on how firms can work effectively with their suppliers to test and build the resilience of their important business services.

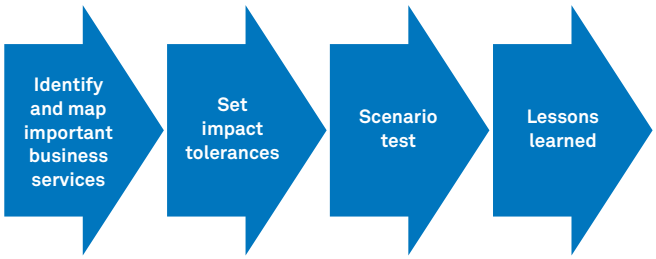
Section 9 focuses on the practical considerations for firms when it comes to logistics and planning, such as who should be present and appropriate meeting lengths to conduct the scenario test. Further to this, the next step for firms is the execution of the scenario tests and more detail on how firms can go about this is included in **Section 10**.

Following such tests, firms will also need to form reports detailing their learnings, what went well and what did not. **Section 11** focuses on how firms can form reports and the main questions they should be asking in these. A deep dive into how firms can approach prioritising remediation activity for any vulnerabilities identified is included in **Section 12**. The final **sections 13** and **14** detail a checklist of lessons learned considerations following scenario tests and suggestions of how to write these up in a Self-Assessment.

2.1 PRE-REQUISITES

In order to progress with scenario testing, a firm will need to have identified its important business services and set one or more impact tolerance(s) for each of these. The IA has previously published industry guidance on important business services, impact tolerances, as well as internal governance arrangements which we invite readers to refer to before they begin scenario testing.

When it comes to impact tolerances, scenario testing plays an important role in validating the intolerable harm threshold set.



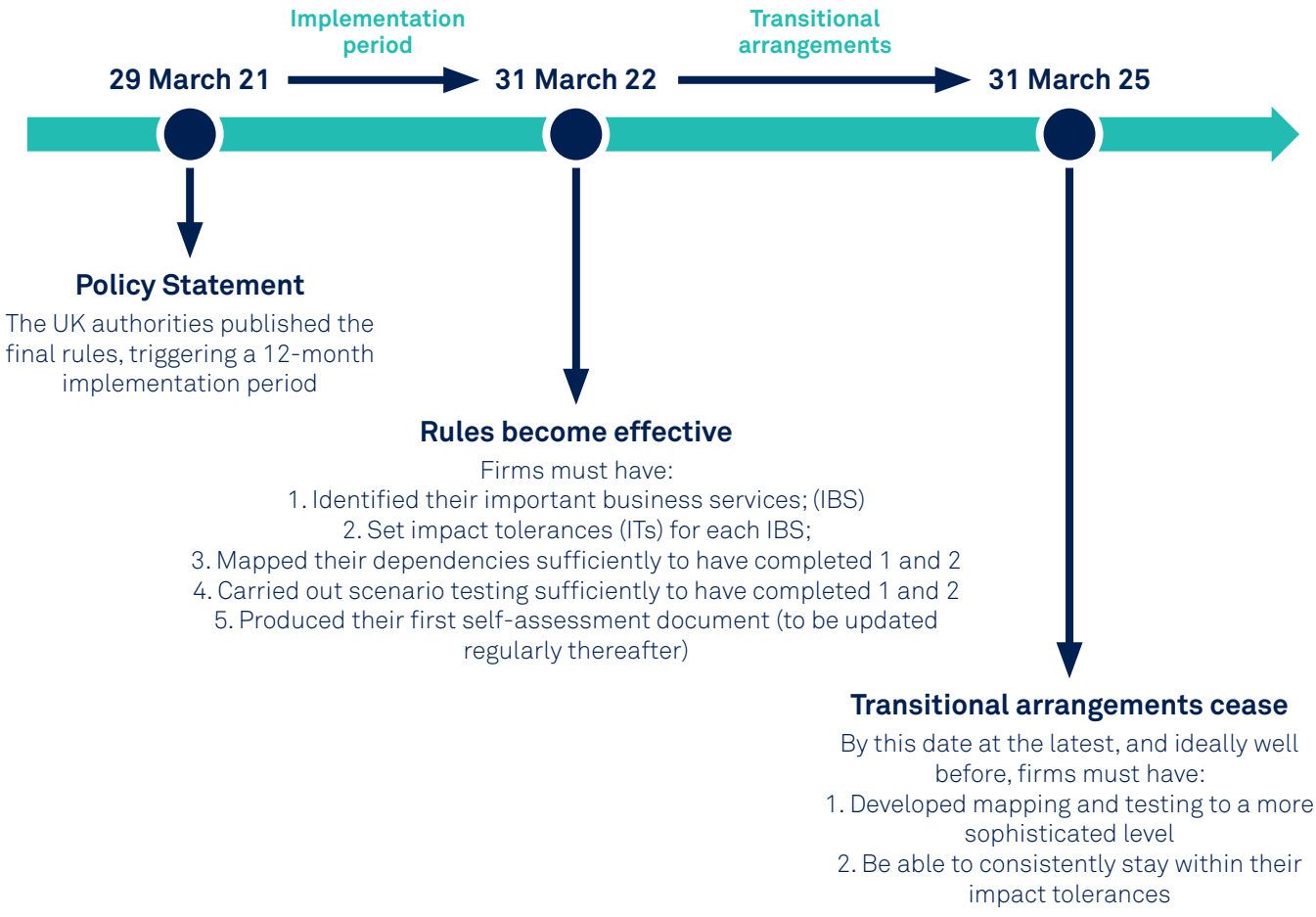
Maturity over time

Firms should expect to build their maturity and the sophistication of their scenario testing over time. We recognise that many firms will be at different levels of maturity at the date of publication of this paper and we look to address this throughout the paper. We offer suggestions for firms who are nearer the beginning of their scenario testing and how they can build their testing sophistication over time.

3. REGULATORY REQUIREMENTS

The publication of the FCA's policy statement in March 2021 outlining their final rules and expectations for firms triggered the start of a 12-month implementation period for firms. By 31 March 2022 firms are required to carry out mapping and scenario testing to a level of sophistication necessary to accurately identify their important business services, set impact tolerances and identify any vulnerabilities in their operational resilience. Whilst firms will not need to have performed scenario testing on every important business service by this date, firms will need to evidence that they have a testing plan in place to be able to increase the level of sophistication of their testing over time.

Firms will then have until 31 March 2025 to continue performing scenario testing with a view to being able to consistently remain within impact tolerances for each important business service.



3.1 SUMMARY OF RULES

Firms need to carry out scenario testing to assess their ability to remain within their impact tolerance for each of their important business services in the event of a severe but plausible disruption.

Firms should ensure that their approach to testing and determining scenarios has received appropriate challenge from senior management and receives their endorsement.

Testing plan

Firms will need to develop and keep up to date a testing plan that details how it will assure itself that it can remain within the impact tolerances for each of its important business services over time. Testing must also inform a firm's view of the scenarios where it would breach its impact tolerance. These scenarios must be reviewed and agreed by the firm Board as part of their Self-Assessment as a minimum.

Firms will need to have a framework in place outlining their approach to conducting scenario tests. In particular, firms will need to consider how they have determined their criteria for formulating severe but plausible service-specific tests (including factors that may complicate a firm's recovery). As part of their testing methodology, firms should also consider the availability of workarounds and substitutes.

Scenario library

Firms will need to have put together 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 important business services in those circumstances.

Scenario test reporting

A firm will need to document the instances when they have remained within their impact tolerances as much as those instances where they have not.

Testing frequency

The FCA have clarified that whilst scenario testing does not need to be conducted annually, firms should test regularly, particularly when there has been a material change to the firm's business, its important business services, associated impact tolerances and to test any remediation activity/improvements the firm has undertaken following a previous test.

The full detail of the scenario testing rules that SM&CR enhanced firms must comply with are included in **Appendix 1**.

3.2 INTERNATIONAL REGULATORY CONTEXT

Whilst the UK have been at the forefront of driving changes in firms to build their operational resilience, there has been significant regulatory interest internationally as well. Scenario testing remains a common theme throughout, with regulators placing an emphasis on ensuring firms test their ability to withstand operational disruption.

- The **Basel Committee for Banking Supervision** (BCBS) *Principles for Operational Resilience* has a different emphasis to the FCA. They do not look at stress testing individual business services but rather suggest banks should have business continuity plans in place and conduct business continuity exercises under a range of severe but plausible scenarios in order to test their ability to deliver critical operations through disruption.

- The **European Commission** published a legislative proposal for a *Digital Operational Resilience Act* (DORA) in the EU financial services sector. This proposed regulation is currently working its way through European Parliament and Council and remains focused on ensuring the financial system has the right safeguards in place to withstand information and communications technology (ICT) related disruptions and other risks. They outline that firms in scope should implement a proportional and risk-based digital operational resilience testing programme, including testing critical ICT systems and applications annually.

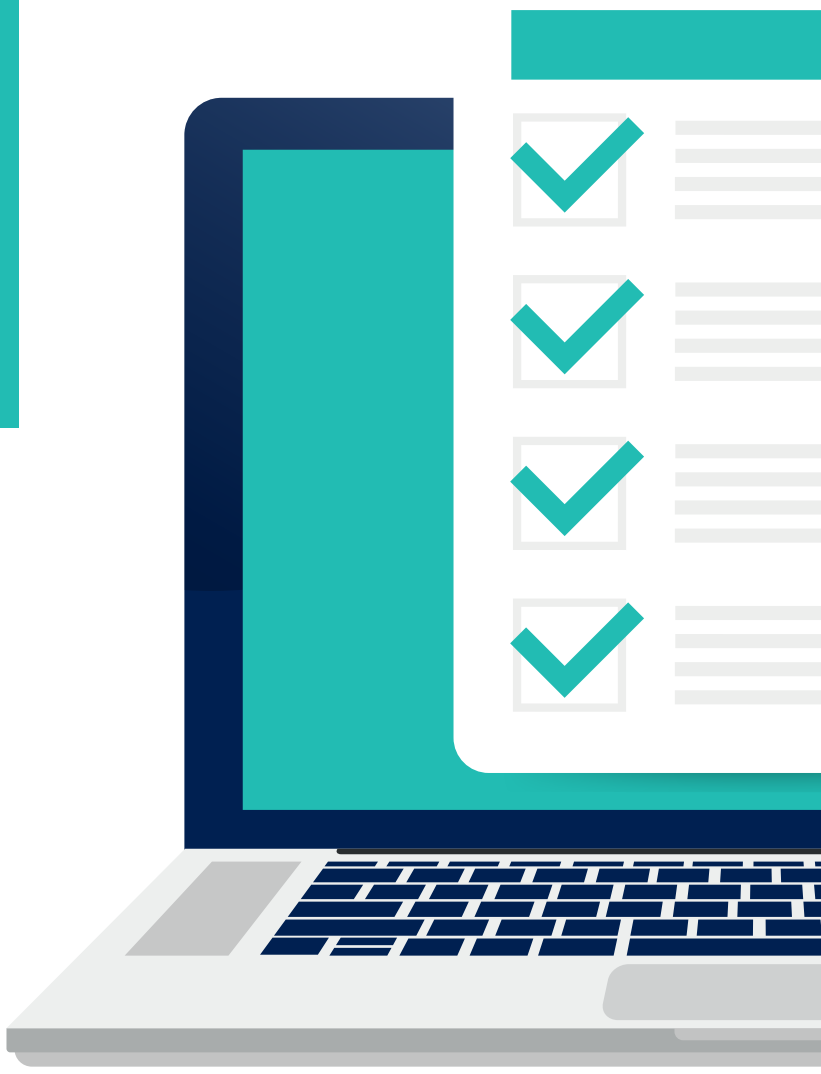
- The **Central Bank of Ireland** has issued *Cross Industry Guidance on Operational Resilience* in December 2021. Similarly to the UK regulators, the Guidance expects that a firm should document and test its ability to remain within impact tolerances for every important business service through severe but plausible scenarios.

4. CREATING A TESTING PLAN

Firms will need to include a testing plan as part of their wider strategic resilience plan. This can include how firms intend to build the sophistication of their scenario testing activities/plans over time. There is an expectation that as firms grow in maturity, their scenario testing plans should develop accordingly.

The FCA requires firms to involve a number of factors in their testing plans:

- **the type of scenario testing undertaken e.g. paper based, simulations or live tests**
- **the scenarios which the firm expects to be able to remain within their impact tolerances and which ones they may not**
- **testing frequency**
- **number of important business services tested**
- **availability and integrity of supporting assets**
- **communication plans**



5. DESIGNING SERVICE-SPECIFIC SCENARIO TESTS

5.1 CREATING A SCENARIO LIBRARY

A scenario library acts as a repository for generic, real-life severe but plausible scenarios that can be used to design business service-specific scenario tests. The scenarios contained within this library benefit from taking into consideration the known risks and threats affecting the firm's important business services, the firm itself and the wider market. The scenario library should be regularly reviewed and updated to reflect the latest risks identified from a firm's broader horizon scanning activities and intelligence gathering exercises.

Having a scenario library provides a framework through which business service-specific scenarios can be developed and relevant complicating factors added to ensure they meet the necessary 'severe but plausible' criteria.

Ownership

The individual with responsibility for overseeing the scenario library will vary according to how firms have defined their governance arrangements, but it will typically be owned by the Head of Operational Resilience and maintained centrally within the resilience function. It may be informed by other teams such as Business Continuity, Disaster Recovery, Operational Risk, Incident Management and IT functions. The key point is to have a central scenario repository that the Operational Resilience teams can feed into, thus ensuring that testing is conducted through a business service lens and captures data around recovery within associated impact tolerance(s). The library should be included in the firm's Self-Assessment, reviewed and signed-off on a regular basis.

Ultimate responsibility is held by those performing the SMF24 function, who should have oversight of operational resilience. If firms do not have an individual performing the SMF24 function under the SM&CR, they must determine the most appropriate individual within the firm who is accountable for operational resilience.

The FCA stipulate 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

Scenario sources

In addition to the 5 scenarios outlined by the FCA, firms can leverage a range of existing sources to inform the creation of a scenario library, these include:

- Actual incidents and near-misses for the firm/its peers and the industry
- The Internal Capital Adequacy Assessment Process (ICAAP)
- *IA Risk Radar* (updated quarterly by the IA's Business & Enterprise Risk Committee)
- National Risk Register (UK Government)
- Business Continuity Institute (annual horizon scan)
- ORX incident database
- Internal, firm specific risk registers
- Cyber Security Information Sharing Partnership
- Global Risk Report from World Economic Forum
- National Cyber Security Centre

Mapping

It is of benefit for firms to leverage the work done to map their underlying resources (the people, processes, technology, facilities, third parties and information) that support the operation of their important business services to help them construct scenarios that test their overall resilience. Understanding the resources in place, and where firms rely upon third party providers for the delivery of their important business services, helps ensure that firms can be better informed to test their contingencies and the potential impact if one of these elements was unavailable.

ICAAP scenarios

Many firms will already be familiar with stress testing for other business purposes. For instance, firms may want to leverage scenarios or processes they have created for their internal ICAAP stress testing programmes. It is often of benefit to leverage existing testing models to fulfil the regulator's expectations for firms to test their ability to remain (or not) within the impact tolerances set for each important business service. However, when utilising existing frameworks, it is also necessary to apply an operational, business service lens.

5.2 EXAMPLE SCENARIO LIBRARY

Pillars	Primary Scenarios
Operational crisis management	Inability to deal with multiple significant incidents
	Failure of infrastructure to manage a crisis
People	Mass staff absence
	Lockdown
Supply Chain & Processes	Material outsourced service provider failure
Technology & Information	IT Infrastructure Failure
	National Infrastructure Failure
Facilities	Loss of premise supporting key workers
Cyber & Fraud	Large Scale Cyber Attack
	Large Scale Fraud

Under each primary scenario, firms can consider a range of sub-scenarios to test. For instance, firms may want to consider under IT infrastructure failure, the impact of a mass data centre failure on their important business services.

In order to ensure a firm's scenarios are severe enough to meet the regulatory criteria, firms can look to add complicating factors. These could include:

- Multi-location disruption
- Concurrent scenarios
- Periods of high customer/business volumes
- Peak periods (e.g. tax y/e)
- Data loss/integrity issue

5.3 SERVICE-SPECIFIC SCENARIO TEST DESIGN

Once firms have a library of scenarios, they can use these to design business service-specific scenario tests.

Purpose and scope

It is useful to agree the purpose and scope of any test at the outset, this could include factors such as:

- Validating one or more important business service's impact tolerance.
- Understanding whether or not an important business service's impact tolerance would be breached based upon a particular severe, but plausible scenario.
- Testing the aggregate impact of disruption on multiple important business services.
- Testing the suitability of contingency measures firms have in place to recover the service within impact tolerance.
- Testing how the firm would respond to known vulnerabilities associated with any of the assets mapped to an important business service.

Tailoring a scenario to a service

There are many ways firms can create their own service-specific scenarios. What remains important is to ensure the scenarios are designed to be severe yet plausible i.e. understanding the impact a scenario could pose as well as the likelihood of this occurring.

One approach is for firms to decide upon the important business service(s) to be tested, the scenario from the scenario library to be used and whether complicating factors are needed. The scenario can then be tailored to the service, informed by their mapping outputs; mapping helps identify where points of failure and other risks lie in the underlying provision of the important business service and these should be integrated into the scenario test. The test design could consider upstream/downstream service dependencies and any known vulnerabilities which can be exploited. Alongside any complicating factors, the scenario's severity can also be enhanced by considering existing recovery time objectives (RTOs), Business Continuity/ Disaster Recovery plans, and known contingencies. By considering these other factors, firms can have an informed view of how severe the scenario needs to be in order to really test the ability of the firm to withstand disruption to its important business services.

It should be noted that understanding the scenarios where a firm would be out of tolerance can be just as useful as understanding those where they would not be. These are helpful to determine areas where adjustments need to be made or understand areas where a degree of risk acceptance is needed.

Can firms carry out some tests that just test their ability to recover within RTO?

By conducting scenario tests that just test their ability to recover within RTO, firms can miss the opportunity to stress and identify the point of intolerable harm which will likely materialise at a different point to a firm's RTO. A scenario test needs to be severe enough to really test the ability of the firm to recover the service within impact tolerance. The likelihood is that the impact tolerance will be longer than the RTO, so the scenario therefore needs to also reflect this longer duration.

Firms can choose to perform supporting tests such as for contingency planning that can be less complex in nature. As firms mature, they will be able to increase the sophistication of their tests.

Climate change risk

Climate change related events such as severe weather events can be considered severe and plausible scenarios. Undertaking analysis into a firm's vulnerability to flooding for instance can help inform a firm's approach to resilience and inform their testing strategy.

Firms may also want to consider the impact of the physical risks of climate change on their supply chains and how this may impact the delivery of their important business services.

Group service testing

A group service typically involves the provision of services by another legal entity e.g. a shared service centre. This will usually include services provided to clients but may not solely be within the legal entity's control. Group services will need to be tested where they play an integral part of the important business service provision.

6. SCENARIO TESTING OPTIONS

There are a variety of methods firms can take when conducting scenario tests. The type of test chosen will likely depend on the maturity of firms' business service management frameworks and their appetite for full end-to-end service scenario tests. For those less progressed, they may wish to opt to utilise asset based rather than full service scenario tests in the first instance.

Some key considerations firms can bear in mind:

- The format and participants of scenario tests are service dependent.
- Consider testing the potential aggregate impact of disruptions to multiple important business services in a single test.
- Consider testing important business services as well as firm-wide scenarios.

6.1 ASSET BASED Vs FULL SERVICE SCENARIO TESTS

It is important to run tests holistically, engaging the whole business to focus on how to continue to provide a service and prevent harm to consumers, rather than focussing on the underlying assets/cause.

It is important to recognise that testing services end-to-end requires a significant **shift in mindset** and emphasis. Nonetheless, firms will need to work towards building their testing capability to be able to assess their end-to-end resilience in order to fulfil the regulator's expectations. Whilst asset-based testing may be completed initially, and likely continue as part of the Business Continuity/Disaster Recovery programme, all firms should consider whether it is appropriate for them to progress towards service testing over time.

ASSET BASED TESTING

'Asset' in this context refers to resources (the people, processes, technology, facilities and information that support the delivery of a firm's important business services). An asset based test would look at an outage of an essential resource that is crucial to the delivery of an important business service and assess its resilience.

An asset based test validates the viability of the associated workarounds and understanding the root-cause of the outage. This type of test does not necessarily have a service lens or address the potential to cause harm.

END-TO-END SERVICE TESTING

A service based scenario test focuses on the relevant playbooks, workarounds and substitutes to assess whether an important business service's impact tolerance would have been breached and intolerable harm caused.

Asset based testing differentiates from service based testing as it is cause orientated, while service based testing considers the impact of disruption.

Full service testing can be challenging to conduct and as such many firms would likely need to mature their processes before achieving this stage and look to achieve full service tests over time.

6.2 DESKTOP WORKSHOPS TO LIVE TESTING

Scenario tests can take a wide variety of formats and selecting the most appropriate will be informed by the maturity of the firm's operational resilience programme.

Drill

For firms lower down the operational resilience maturity scale, they may wish to utilise drills. These are typically informal, team-based exercises that test at the asset level. The main objective is to run through roles and responsibilities.

Simulated, stressed scenario test (internal)

Firms can look to conduct facilitated, simulated tests involving both business and functional stakeholders. These should test their response to a severe but plausible incident affecting an important business service, leveraging injects and other stress techniques. These can utilise data from incidents or near misses to test the viability of workarounds to assess the impact on the end-consumer.

Full live test

A full live test involves creating a real-time disruption and testing the firm's ability to remain resilient and within impact tolerance. This is typically conducted in the production environment and tests how the firm can continue to be deliver that important business service through disruption.

Incident

Whilst not a test, real-life incidents can help a firm determine the effectiveness of its resilience measures. Data from incident investigations can also be repurposed to inform desktop assessments, particularly regarding any vulnerabilities that have been exposed and how long it would take to detect an issue.

Desktop workshops

Scenario-based workshops can be a useful and less resource intensive method to conduct testing. These tests typically involve management and third party providers (where possible). These can be structured based upon questions focussed on walking through the steps of a BCP or crisis management plan.

Depending on whether the scenario in question is sufficiently severe and complex, it can be a useful tool to assess impact tolerances.

Simulated, stressed scenario test (Involving third party providers)

It is of great benefit to firms to be able to coordinate testing with their material third party providers crucial to the delivery of their important business services. There are specific factors to consider such as testing exit strategies. However, this can be difficult to facilitate in practice as we discuss later.

Live parallel test

Whilst live tests can help to determine where consumer harm will manifest, the sorts of scenarios a firm may have the appetite to test live are probably less severe than in a simulated exercise. By contrast, 'live parallel tests', where firms do not disrupt their production but rather test their contingency arrangements, are a useful alternative and less risky than a full live test.

Parallel tests still involve real-time testing but instead of focusing on disrupting the service delivery, they are centred on the viability of the firm's contingency arrangements.

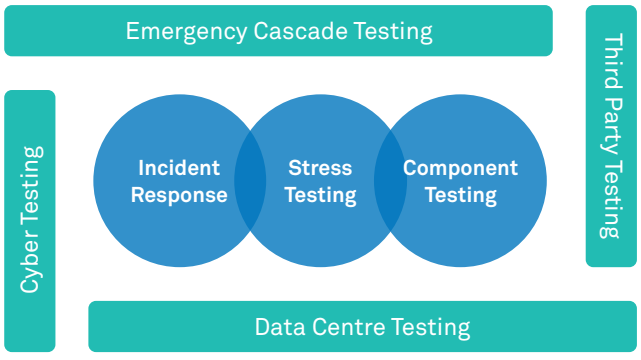
Impact of testing on business as usual (BAU) operational needs

In PS 21/3, the FCA clarified their expectations on how testing requirements will impact on BAU operational needs. Whilst they recognise that firms may face resourcing issues and other operational concerns that may affect the functioning of BAU activities, the FCA stipulate that firms should factor these concerns in when conducting tests and consider how best to minimise disruption to other activities.

Firms will need to be able to justify what level of testing they have chosen and evidence that they have a scenario testing plan in place for all their important business services that would grow in maturity.

6.3 AN INTEGRATED APPROACH TO TESTING

Firms can take an integrated approach to testing looking to mature the related component parts including incident response, stress testing and component/contingency testing/testing against RTOs, supported by other tests such as communication plans.



Stress testing remains an important facet and firms can also look at how they can integrate their testing with operational risk functions. All testing layers are measuring a different aspect and firms should look at all the different elements with a maturity lens and seek to build their sophistication over time. Business continuity and other testing are all still important, but it is important to recognise that scenario testing has a specific focus on 'intolerable harm'.

Area of challenge: determining and testing aggregate harm when multiple business services are disrupted

The regulators emphasise that firms will need to consider the impact of aggregate harm when multiple business services are disrupted, such as in the event of a ransomware attack. It can be hard to determine intolerable harm in these situations as many business areas would be unaffected, but some would not be.

Taking a data driven approach to identifying a firm's important business services can help firms identify which services are most important in a business. Service tiering can be helpful to understand which services are the most important so that when testing, firms can focus on bringing back the services that have the potential to cause the greatest harm. In addition, firms need to understand the interconnectivity between services to help inform their answer to determining aggregate harm and the order in which business services should be recovered.

Understanding the sequencing of events when disruption occurs is also important to understand which important business service firms should prioritise first to prevent harm materialising. This may not always be the most obvious service as it largely depends on where disruption occurs. It was also noted that looking at sequencing across group businesses and understanding the underlying dependencies and where intolerable harm would appear is far more challenging.

7. COLLATING DATA TO INFORM SCENARIO TESTS

Having the right data and data sources in place is important to be able to design service-specific scenario tests that are severe enough to appropriately stress the impact tolerance. In simple terms, the more data firms can utilise, the more plausible their scenario tests will be.

WHY DO FIRMS NEED DATA?

There are numerous reasons why firms benefit from optimising the data at their disposal to inform their scenario testing. These include:

- Having a rich set of vulnerability data enables firms to stress known vulnerabilities, increasing the severity and plausibility of the scenario. Leveraging historical incident-related data can be particularly helpful in this regard.
- Historical data also helps those participating in the test, who may not be familiar with the service being tested, become more acquainted with how the service operates.
- Having performance data related to their important business services helps stakeholders understand the business service in more detail as well as their critical break points and ensures efforts are directed to plug these vulnerability gaps.
- Good data can help the business predict what workarounds/substitutes and action plans may be invoked during the scenario test and therefore ensure these are also factored into the design of the actual scenario test.

Ultimately, having good quality data in place to support the design of scenario tests helps to assess a firm's preparedness for a service disruption.

EXAMPLES OF DATA TO BE GATHERED WHEN DESIGNING A SCENARIO TEST

There are a variety of data types that firms can use to inform their scenario testing and design severe but plausible tests. For instance, if a firm understands what their usual BAU capacity for trades is, they are better able to determine what would be a significant enough disruption that could cause potential harm to consumers. A rich data set helps to ensure the scenario being designed is as realistic/plausible as possible, but also as severe as a firm can make it, based upon the data points gathered below.

1. Important Business Services and Mapping

Firms can leverage the metrics used to determine the importance of the business services they identified as a scenario testing data source. Likewise, conducting mapping helps to identify upstream/downstream service resource dependencies that can also be used to create severe but plausible scenarios. Moreover, firms can consider the resilience and vulnerabilities of the underlying resources themselves involved in supporting the delivery of the important business service.

Examples include:

- To identify a firm's important business services, firms may have utilised scoring criteria to determine how a service would impact the customer, firm and wider market, should that service be disrupted. The metrics involved can be leveraged to inform the firm's scenario testing.
- When conducting end-to-end mapping, firms can identify a range of data points that can inform a firm's scenario testing including:
  - The resources that are critical to the continuing delivery of the service.
  - The third parties involved in the value chain and any interdependencies.
  - The services and underlying systems needed to keep the business running on a day-to-day basis and therefore deliver the entire important service.
  - The digital dependencies involved in delivering a business service for instance internet connectivity and IT systems.
  - Single points of failure across services such as underlying IT software.

2. Impact Tolerances

Incorporating the data used to justify the level firms set their impact tolerances and how intolerable harm would materialise, can help ensure that the scenarios being tested are severe enough.

Whilst setting impact tolerances will likely involve a combination of judgement and data led approaches, relevant data points include:

- Leveraging existing data to establish a baseline for the day-to-day functioning of the service. By doing so, firms can understand how delays to the normal delivery of the service can manifest in harm.
- Typical time frames where harm could occur.
- Complaint levels and volume of client contact.
- The important business service's estimated time to recovery.
- Utilising proxy measures for harm, or conduct primary research to better understand the potential harm to consumers.
- Examining contractual obligations where harm would arise out of a failure to meet that agreement.

3. Operational data

Using the existing operational data at firms' disposal is of great value to inform the design of scenario tests.

Examples include:

- System performance data.
- Data around facilities management (e.g. how long it would take to relocate staff).
- Availability of back-ups/workarounds and the time to invoke (what would the impact be if these are not available).
- Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
- Duration to failover.
- Data recovery times.
- Risks, Issues and Audit Points including relevant outputs of Risk Control Self Assessments and Supplier Oversight / Due Diligence Tasks.
- Contingency procedures and timeframes as identified in Business Continuity Plans and Disaster Recovery Plans relevant to the important business service(s).

4. Volumes

Details on the transaction or service volumes, including peak volumes, is useful to gather. In particular, firms can consider their BAU volumes (how much do you typically process on any given day) and BAU capacity. Firms may also wish to utilise historical market data to understand past peaks and troughs that impacted their service delivery.

Examples include:

- Number of transactions during low and peak periods to help identify pinch-points.
- Capacity to process transactions per hour.
- Average value of transactions.
- Average number of customer calls per day.
- Impact of planned new product ranges on existing volumes.

5. Third parties

Firms should have knowledge of the Service Level Agreements (SLAs) with any third party providers/ teams undertaking critical parts of the important business service. In particular, firms should understand the responsibilities of all involved in the delivery of an important business service. This data set would be even more valuable if firms are able to coordinate testing with their third party providers.

6. Past incidents and near-misses

Historical incidents/near-misses, including data from Risk and Incident Management systems, provide a useful data set and an insight into a firm's vulnerabilities. Information gleaned from previous incidents can also help firms understand how quickly an issue would be detected.

7. External data

Firms can also utilise a range of external events data relevant to the chosen scenario. This can be informed by operational risk horizon scanning. Examples of external data sources are included under **Section 5.1, Scenario sources.**

8. Consumers

Consumer numbers and analysis of the cohort relying on the service is an important dataset to capture to inform a firm's scenario testing. Other consumer-related data that is useful includes existing contractual arrangements with clients (e.g. identifying specific timelines for service delivery that if breached would cause harm). It is worth remembering that intolerable harm constitutes harm from which consumers cannot easily recover e.g. where a firm is unable to put a client back into a correct financial position, post-disruption, or where there have been serious non-financial impacts that cannot be effectively remedied.

Area of challenge: gathering consumer harm data

Gathering data regarding where consumer harm can manifest can be difficult to collect, however there are a few approaches firms can take:

- **Previous incidents:** looking at previous incidents offers useful data and can help firms identify where harm to consumers manifested. In particular, analysing incidents where consumers were paid compensation can help the firm to understand what went wrong, what caused the firm to pay compensation, where consumer harm occurred and if there were any knock-on effects. It is important to note that where a consumer is paid compensation and has not been impacted further, it is unlikely that intolerable harm would have been caused. Firms should understand the sorts of customer impact which materialised as a result of the service disruption through their previous incident analysis.
- **Hearing directly from consumers:** sending a questionnaire to consumers to hear directly from them what services they consider most important and how long they can cope without these services can be useful. Feedback from this questionnaire can then provide evidence for the firm's methodology and help the firm better understand potential harm points. Likewise, some firms set up consumer focus groups rather than trying to second guess what consumer harm would look like.

It can also be useful to look at other sectors and the different types of consumers that experience disruption. Firms should recognise that harm may materialise differently depending on the consumer type on the receiving end of the important business service.

Having a plan or playbook is not sufficient by itself, firms will need to be able to test using service-specific data to build their resilience. Scenario testing data and outputs will provide senior management with more confidence and help identify vulnerabilities and any required remediation activity.

DATA ADJACENCIES

Data being collected by firms to help build their operational resilience can have a wider utility beyond its intended use. Some of the data collected by the firm to inform their scenario testing can be used to provide new insights into other projects and regulatory change programs the firm is implementing.

Other datasets identified in the mapping and scenario testing process can help support the business case for strategic change. For instance, any vulnerabilities identified through scenario testing may encourage the business case for moving to the cloud or provide the justification for increased or reduced outsourcing. This is discussed in more detail in **Section 12** on remediation.

8. THIRD PARTY RISK MANAGEMENT (TPRM) TESTING REQUIREMENTS

8.1 REGULATORY REQUIREMENTS

FCA expectations on testing with third parties

Firms are expected to work 'as effectively as possible' with third parties involved in the provision of their important business services to ensure the firm can remain within impact tolerances. Regardless of their dependence on third parties, firms will retain ultimate responsibility for ensuring they meet the FCA requirements.

The FCA have their own TPRM considerations inherent in their rulebook. They expect firms that utilise third party providers to take reasonable care to organise and control their affairs responsibly and effectively, with adequate risk management systems in place (Principle 3 in their Handbook).

When it comes to scenario testing, firms may wish to coordinate with their material third parties to create realistic scenarios. However, it may not always be easy to do so particularly if third and fourth parties become overburdened by testing requests. The FCA are very clear that regardless of how firms choose to conduct testing, it remains the responsibility of the firm.

Firms in scope of the policy will need to satisfy themselves, if the third party is going to carry out any testing, of the methodologies, scenarios and considerations of the third party in doing so. The firm is ultimately responsible for the quality and accuracy of any testing carried out, be that by themselves or by an external party. ***FCA PS21/3***

Existing regulation

There are number of existing or parallel pieces of regulation that have been published or are being developed that the FCA encourages firms to have regard to the:

- EBA Guidelines on ICT and security risk management (EBA/GL/2019/04) and the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02).
- BCBS' proposed Principles for Operational Resilience and the European Commission's proposed Digital Operational Resilience Act (DORA).
- Recovery and Resolution Planning (RRP), Operational Continuity in Resolution (OCIR), Resolvability Assessment Framework (RAF) and business continuity planning (BCP).
- International Organization of Securities Commission's (IOSCO's) Principles on Outsourcing.
- SYSC 8 Outsourcing requirements.

Dual-regulated firms

Firms regulated by both the PRA and FCA will need to comply with Policy Statement 7/21 (PS7/21) and Supervisory Statement 2/21 (SS2/21) by 31 March 2022. These were issued as part of the wider operational resilience policy package released by the regulators earlier in 2021. However, even for those who are not in scope, it is also helpful to consider some of the rules outlined regarding TPRM and outsourcing. With regard to testing, the PRA stipulates a number of requirements for firms:

- **Business continuity:** the regulated entity and service provider should test their business contingencies plans.
- **Exit strategies:** firms should test their exit strategies and in particular, those relating to stressed exits.
- **Sub-outsourcing:** the regulated entity should ensure the that the service provider has the ability on an ongoing basis to appropriately oversee any material sub-outsourcing, including establishing that the service provider has in place robust testing, monitoring, and control over its sub-outsourcing.
- **Intra-group outsourcing:** firms should have appropriate monitoring and oversight of their intragroup outsourcing arrangements; for instance firms should understand their reliance on group shared services and ensure they can withstand disruption to these. Intragroup outsourcing is subject to the same requirements and expectations as outsourcing to service providers outside a firm's group and should not be treated as being inherently less risky (however the regulators do recognise that control and influence may vary depending on the characteristics of a group).

8.2 WORKING EFFECTIVELY WITH SUPPLIERS

Many firms will utilise third parties as part of their end-to-end important business service provision and others will outsource some of their important business services entirely. In either case it is important to work effectively with suppliers to build a firm's operational resilience. This includes working with suppliers on setting/agreeing impact tolerances, conducting mapping/identifying vulnerabilities, scenario testing and any associated remediation work.

Setting impact tolerances

The FCA expects firms to be able to set and, in time, remain within their impact tolerances regardless of whether it uses external parties for the provision of its important business services and expects firms to work effectively with that provider to do so.

1. As a first step, firms will need to identify the third parties that support their important business services and identify which to prioritise and engage with. Firms can choose to review the outsourced provider's obligations via their SLAs.

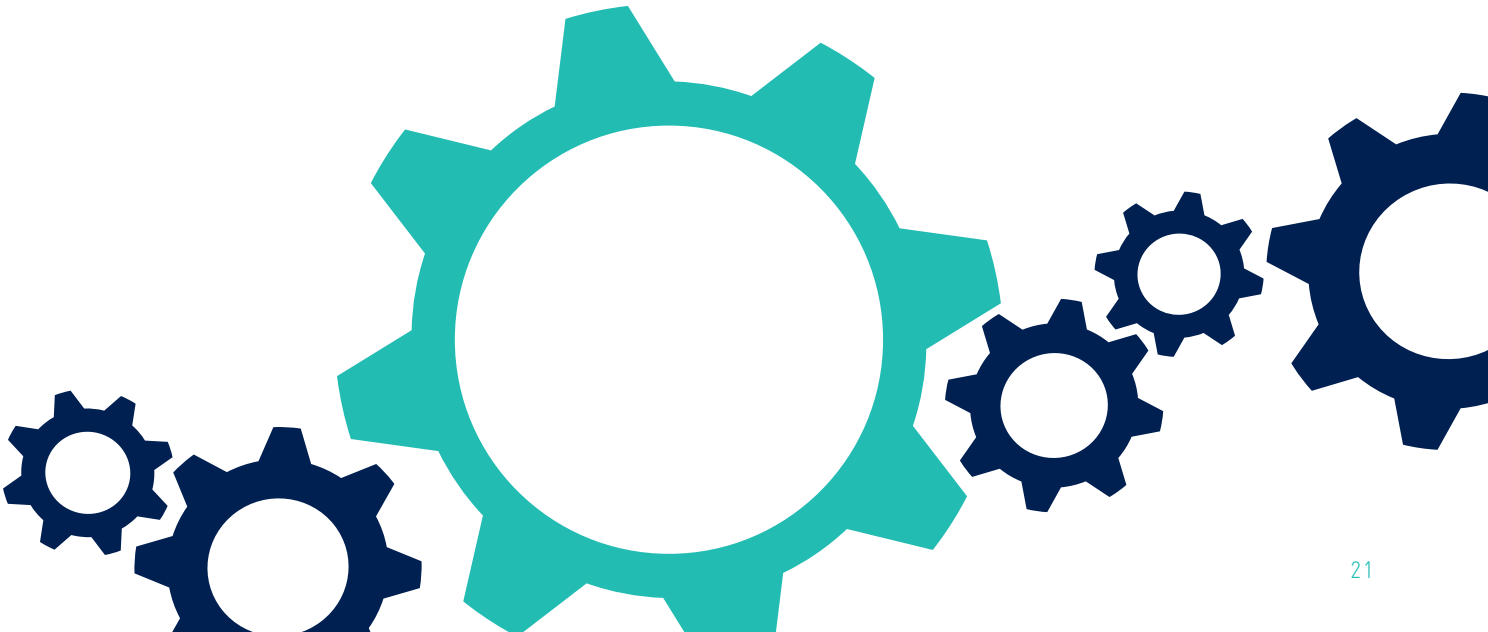
2. It is useful to calibrate impact tolerances with any third parties involved in the provision of a firm's important business services to be able to ensure the supplier's impact tolerance is no longer than the one their client has identified. As such, proactively engaging with third parties early, sharing approaches to setting impact tolerances and initiating discussions on what 'intolerable harm' constitutes is important.

3. Firms will need to gain comfort that any third party provider(s) involved in the delivery of their important business service can recover within the impact tolerance defined by the regulated firm. It is the expectation of firms that for important business services which are wholly outsourced, these service providers will be expected to share more information with the regulated firm. By contrast, where a third party supports the regulated firm in only part of the provision of its end-to-end business service, it is likely that the insights the third party needs to share with the firm regarding whether or not an impact tolerance would be breached, would be more limited.

The Working Group noted that many providers may not know that they have been identified as crucial to the delivery of an important business service and that this should be communicated to them. For instance, market data vendors and multi trading facilities.

Some providers may well be regulated themselves and so will also be working on operationalising the regulatory requirements, making it easier to initiate conversations on testing/assurance. However, for those that fall outside the regulatory perimeter it can be more challenging.

Outsourced providers can also help firms with their benchmarking as they may have greater visibility of how multiple firms are setting their impact tolerances and so be able to identify which firms are outliers in terms of their tolerance levels.



8.3 SCENARIO TESTING OPTIONS WITH THIRD PARTIES

There are a number of ways firms can go about testing the ability of their important business services that they have either wholly or partly outsourced to remain resilient in severe but plausible scenarios.

1. **Co-testing:** it can be of great benefit for firms to conduct joint scenario tests with the third parties they rely on for the provision of all or part of their important business service. When co-testing, collaboration is critical. Desktop workshops can be a good starting point as it can be used to generate useful insights at a lower cost (in terms of resource and time).

2. **Assurance:** firms may need to gain their assurance from the results of scenario tests conducted by their third parties. This would ideally include data on the vulnerabilities identified and the remediation plans the third party has put in place, along with details of how the third party will update the firm on the progress of such remediation plans. However, the challenge remains as to how willing the third party is to share such information. Other ways firms can gain assurance by proxy is to look back and consider the experience of previous incidents.

3. **Independent review:** firms may need to gain assurance through independent review if the third party is unwilling or unable to share details of their scenario testing activities with the firm directly.

Firms need to consider testing for both **orderly and stressed exits**. Firms may choose to perform tests looking at the impact of a disorderly exit from a critical supplier from an internal perspective instead of, or in addition to, a joint test involving third parties. Firms should also recognise that a third party may suffer disruption that is recoverable and incorporate this into their testing plan.

Area of challenge: co-testing with suppliers

It can be difficult in practice to arrange co-testing with a firm's suppliers. As such, where possible firms should look to maintain good working relationships in order to facilitate a mutually beneficial solution. As a last resort, firms can look to amend their contracts with their material third parties to introduce a clause to allow for the option of joint testing. From the third party point of view, it was noted that it is highly resource intensive to satisfy all requests for additional information to be provided in contracts and that there is no easy solution.

Whilst it can be of benefit to co-test, firms can also consider the ways they can gain assurance and comfort from the measures third party providers are taking to build their own resilience.

Testing to include fourth parties

Sub-outsourcing, where the third party supplier contracts with a fourth party for part of the service provision, can also produce problems for firms, and they may be constrained by the provisions of existing contracts in the level of access or visibility of the fourth party's actions. Firms will need to work effectively with the third party to arrange scenario tests, taking into consideration the impact of an outage of a critical fourth or fifth party.

8.4 OUTPUTS OF TESTING ACTIVITIES

Firms should document the details of their tests involving third parties including the scenario used, testing method, stakeholders present, actions/ decisions taken and the outcome of the scenario test.

1. Understanding whether or not the firm would have breached their impact tolerance is important to assess. If the firm had not been able to recover their service within impact tolerance, they will need to detail why.

2. Firms will need assurance that any workarounds/ substitutes the third party is able to deploy are resilient. Any vulnerabilities identified will need to be documented along with any agreed associated remediation activities.

Regulators want to understand the scenarios where firms would not be able to recover in tolerance as much as those that firms can recover within. If a firm is not receiving all the relevant information they need from their suppliers, then they can declare this to their Board and state that given a lack of data, they have no confidence they will remain within tolerance for that service. Firms can also flag in their Self-Assessment that they would have liked to have been able to co-test, they were not able to do so and that they intend to improve on this and will continue to build their resilience as the market matures. Ultimately, it is up to the Board whether or not they are comfortable to accept this risk or not.

Area of challenge:
how to satisfy the regulator if a third party is not providing the necessary information/data around scenario testing?

Suppliers may be unable or unwilling to take part in a scenario exercise, let alone share a fully documented report after a scenario testing exercise. It would be more realistic to expect a supplier to provide high level learnings and remediation actions. As a minimum, it is helpful to know if a third party remained within a firm's impact tolerance or not and any remediation activities they are taking.

If the supplier is regulated it is easier to engage suppliers in discussions. If they are not, it is more complicated. Invoking the audit or step-in right in contracts is often unhelpful and largely ineffective in such instances. Firms can try and leverage existing data at their disposal e.g. SLAs although this may not offer enough comfort to firms. Focusing on maintaining a good working relationship, recognising the extra work involved to conduct scenario testing, can be effective ways to gain their cooperation.

9. LOGISTICS AND PLANNING

From a logistical point of view, the test should be well structured and governed appropriately.

LOGISTICS

There are a number of logistical considerations to take into account, including:

- **Meeting invites:** it is useful to issue all participants with a meeting invite well ahead of the test, stressing mandatory attendance.
- **Meeting room:** if conducting in-person tests, the room needs to be of sufficient size to accommodate all individuals and equipped with the necessary facilities e.g. whiteboard, screens, conference call function.
  - **Break out rooms:** allowing for the use of break out rooms is particularly useful (whether in person or via video conferencing) e.g. for a small group to test/ formulate communication plans.

ATTENDEES

It is useful to have a broad range of stakeholders in the room to create as realistic a scenario as possible.

Facilitator
A suitably senior individual can be appointed as the facilitator and they should be briefed beforehand on the scenario and impact tolerances to be tested, as well as any inputs to be used.

Representatives from the important business service
The business service owner and those who have in depth knowledge of the dependencies and associated risks should be involved. Other relevant personnel may include members of Technology, Incident Management, BCP, Compliance, Regulatory Liaison, Distribution/ Client relationship, Operational Risk and Operational Resilience teams. Third parties may be necessary where they play an integral role in the provision of the important business service being tested.

Senior individuals
Involving senior individuals in scenario tests including the COO, Non-Executive Director(s) (NEDs) and Board members also helps to provide valuable insights.

Note taker(s)
Documenting the decisions and actions taken is hugely important during scenario testing. Dependent on the resources available to the firm, they may wish to have more than one note-taker to capture all the necessary information.

Area of challenge: should you prepare/brief all attendees in advance of the test?

Members debated the utility of constructing 'insider' and 'outsider' teams whereby the former would include those staff who are knowledgeable about the service and its delivery mechanisms, and the 'outsider' teams would be the key stakeholders to be engaged during the day of the scenario exercise itself. It was suggested that an insider team could be involved in the design of the test to extract the most useful results whereas the outsider team should be excluded from the design and preparation so that the test could be run in as realistic way as possible on the day.

However, upon debate members agreed that at least in year 1, preparing all attendees ahead of time would ensure the best test outcome whilst firms remain at an early stage in their testing. Firms may wish to form briefing packs for those attending to ensure all are clear on the purpose of the exercise and that attendees come prepared with relevant material (such as incident management playbooks, business continuity and disaster recovery plans). Some also noted that it was important that attendees have a good knowledge of the important business service being tested and its resource dependencies as a pre-requisite.

As firms build their maturity, they can look to utilise insider/outsider teams where some attendees come into the test unprepared to ensure they achieve the most realistic scenario tests.

Other considerations

Tests can benefit from not being conducted with the same participants every time in order to achieve a more complete resilience picture (particularly on how different individuals would respond) and also to gather more diverse opinions.

10. SCENARIO EXECUTION

When it comes to executing a scenario test, firms can consider how the session will run and where the test entry point should be.

10.1 PREPARATORY WORK

As we outline from the start, firms will need to test their ability to remain within their impact tolerances for severe yet plausible scenarios. However, over time firms may look to build their sophistication by going beyond specific requirements and conduct reverse stress testing where the firm seeks to find a scenario that will deliberately break the firm's tolerance.

Some firms may wish to conduct a lot of analysis ahead of the scenario test to ensure the scenario is severe and plausible. Firms can leverage existing risk data to identify known vulnerabilities amongst other data points to come up with a scenario timeline outlining the point at which harm would crystallise and use this as a basis to plan a scenario test.

10.2 SCENARIO FACILITATION

The role of the facilitator is to manage the discussion, ensure attendees remain focused on the session objectives and to introduce new injects or complicating events in the scenario to increase its severity as and when appropriate. The facilitator should ask probing questions, particularly around the decisions taken at each stage to assess the impact on the end user. Some considerations firms can bear in mind when facilitating a scenario are highlighted below.

1. **Introduction and objectives**
   It can be useful to detail introductions and the objectives of the session from the outset, with the facilitator providing sufficient context and background information. They should stress that it is important that attendees do not challenge the scenario in order to focus on identifying the potential for harm and any vulnerabilities associated with the service.

2. **Initiate first inject to the scenario and open up for discussion**
   Following the introduction, the attendees can begin assessing the severe but plausible scenario in question and agreeing what actions/decisions they would take. The facilitator should look to introduce new injects when appropriate and ask probing questions.

3. **Assess where harm would manifest as the scenario progresses**
   As the scenario progresses, the note taker should record at regular intervals, based upon actions taken and decisions made, whether the business believes the end user(s) of the service would be experiencing intolerable harm. Those present should continue to assess where harm would manifest to consumers and the market as the scenario progresses.

4. **Wrap-up and next steps**
   Once attendees believe the incident would have been resolved and BAU service resumed, the facilitator can bring the scenario to a close. Attendees should agree on whether the workarounds/substitutes invoked would have been resilient and whether intolerable harm would have materialised. When assessing this, firms may also consider that initial workarounds may not be resilient in the long run (some may only work for 5 days for instance). If the service would not have been recovered within impact tolerance, attendees should consider how long it would take to bring it back.

   Whilst all stakeholders are still in the room, it is advisable for the facilitator to gather feedback and request attendees to give their views on:
   - What went well/did not go well
   - Immediate lessons learned
   - Any enhancements /remediation required
   - Initial assessment as to whether the impact tolerance is appropriate

5. **Scenario report**
   It is useful for firms to produce a report following the test, recording the decisions and actions taken as well as any lessons learnt. This should be drafted and shared with all attendees for review/feedback but ultimately signed off by the service owner and dependent on the organisational maturity of the firm, relevant steering committees.

11. SCENARIO TEST REPORTING

There are a number of different strategies that firms can utilise to collate the outputs of their scenario tests, ranging from spreadsheets to reports. Forming a scenario test report addressing the purpose and outcome of the test conducted is an important step to take forward any learnings/remediation work as well as to form part of the firm's governance process.

Reporting templates
Having a skeleton template in place ahead of the scenario that is then updated through pre-planning, the scenario test itself and after the test has completed is helpful. This can help the individuals involved in developing the test and provide a point of reference/objectives to refer to.

Some considerations to help firms form their reports are outlined below.

Executive Summary
An executive summary can be included at the start, providing an overview of the key points e.g. whether the impact tolerance was breached or not.

1. **Attendees**
   List the attendees present and their roles.
2. **Timeline of how the scenario unfolded**
   Detail the key decisions made and actions taken (and why). Firms can also capture the impact of disruption to the important business service on the end user/market stability/firm viability and whether intolerable harm manifested.
3. **Assessment**
   a. **overview of the workarounds/substitutions invoked** and an assessment of their resilience/ability to continue to provide the service
   b. an assessment as to whether or not the **impact tolerance** would have been breached
   c. an assessment as to whether or not **existing playbooks, Business Continuity/Disaster Recovery plans** are effective and what updates are required
   d. an assessment as to whether or not any **communications deployed** were suitable and what updates are required
   e. participation levels from attendees
4. **Summary of areas of good practice identified**
5. **Vulnerabilities and risks identified and other lessons learned**

OPTIONAL
Dependent on the firm, some may choose to take more time to present a detailed report with a clear remediation action plan whilst others might leave this section briefer to ensure there is a quick turnaround time to complete the scenario report and define a remediation plan later.

6. **(Remediation plans/recommendations**
   To address the vulnerabilities listed, a series of recommendations or plan should be included. This can include owners for ensuring the remediation is actioned, the level of difficulty to implement, due dates, and whether funding has been secured.)

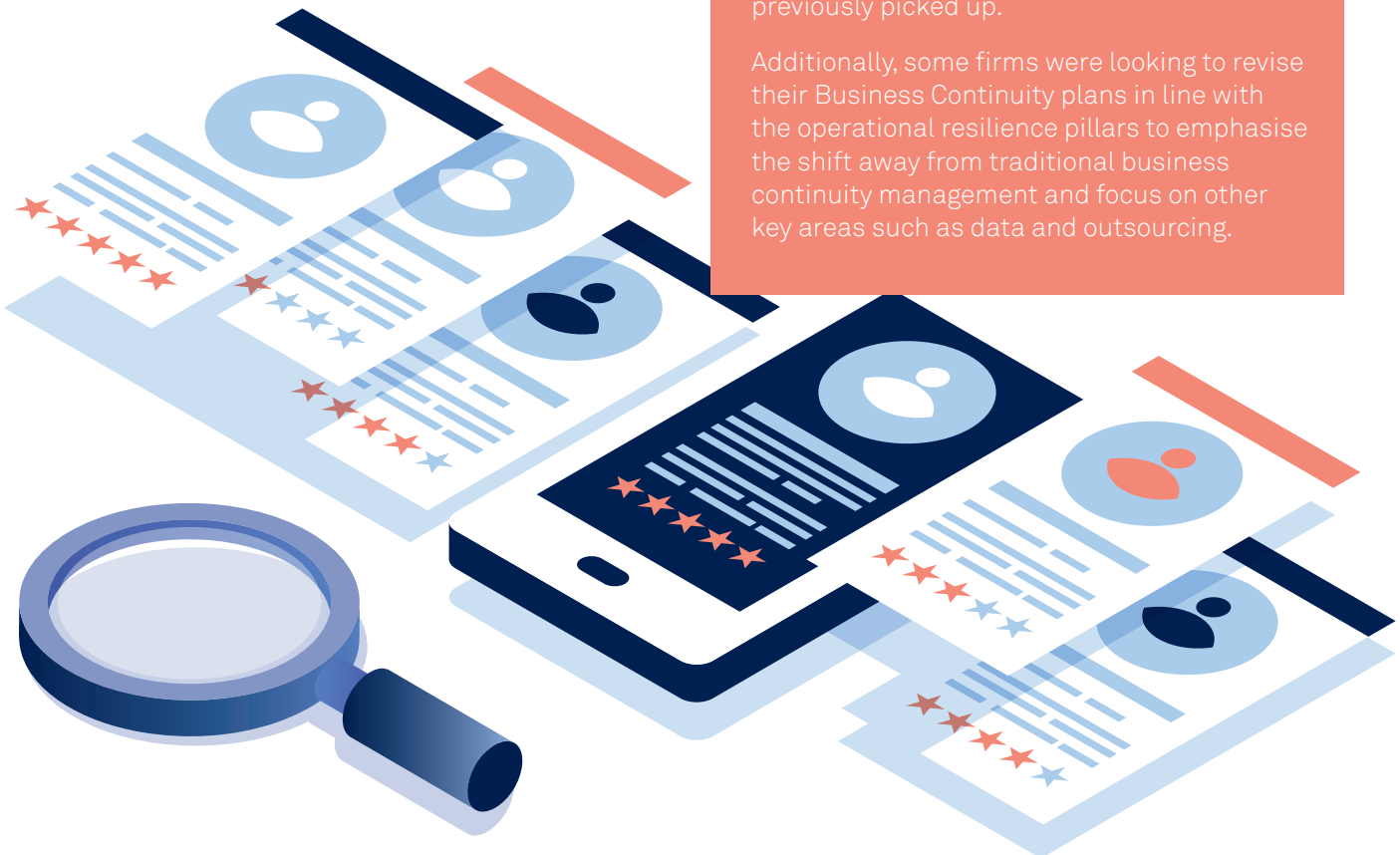
The test report benefits from being shared with as many of the participants as possible to ensure their feedback is captured before it goes through formal governance for final sign-off.

Area of challenge: how do you assess whether existing Business Continuity/Disaster Recovery plans are effective?

Given the variety of operational incidents, a firm's response to each incident will likely differ which can make it hard to assess whether a firm's existing Business Continuity/ Disaster Recovery plans are effective. Firms should ensure that roles are clearly defined and that the necessary steps are unambiguously documented in such plans.

One approach is for firms to review their Business Continuity plans as part of the preparatory work before embarking on the scenario exercise. By undertaking detailed prep work, firms can determine where failures are likely to emerge as part of the scenario timeline and so test these assumptions and identify vulnerabilities that had not been previously picked up.

Additionally, some firms were looking to revise their Business Continuity plans in line with the operational resilience pillars to emphasise the shift away from traditional business continuity management and focus on other key areas such as data and outsourcing.



12. VULNERABILITIES IDENTIFICATION & REMEDIATION

Once the scenario test report has been signed off, firms can look at their remediation planning. For each vulnerability identified, firms will likely need to raise a risk and come up with a proposed remediation plan. The level of detail in such a plan will depend on the vulnerability in question and the data available. When doing so, firms can consider assigning an owner and determine a priority level for the remediation activity linked to whether there is a high likelihood of the vulnerability impacting the ability of the service to recover within impact tolerance.

Vulnerability identified:	
Risk score	
Owner	
Priority (high, medium, low)	
Proposed remediation • Service improvements • Resilience improvements	
Level of difficulty	
Time to implement	
Indicative cost level	
Funding secured?	

DETERMINING A VULNERABILITY OWNER

Remediation activity can be owned by the relevant pillar that was affected/where vulnerabilities had been identified during the scenario test. For instance, if the scenario test had identified technology-related vulnerabilities, the design of the remediation should be owned by technology. However even in such cases, remediation activity should not be conducted in isolation and service owners can be engaged too.

Firms may need to ratify the remediation activity and in some instances re-test to confirm the vulnerabilities have been addressed. In addition, if firms have changed the ways in which they would respond to an incident going forward as a result of their scenario tests, playbooks, Business Continuity/Disaster Recovery plans and communication plans may need to be updated.

VULNERABILITY SCORING

Allocating a score can help to drive immediate focus on the issue at hand. For instance, if a scenario had been deemed to breach impact tolerance and major remediation was required, this would be prioritised. A sample score rating system is included below:

Overall scenario
Expected to remain within Impact Tolerance. No improvement required OR minor actions required.
Likely to remain within Impact Tolerance but may breach in most extreme scenarios. Minor OR Significant actions required.
Likely to breach Impact Tolerance. Significant OR Major remediation required.
Recovery achieved at this point in test.

Firms may wish to also apply a pillar score to help teams specifically locate where the vulnerabilities were identified in the test and so progress with remediation activity.

Pillar score
No improvement required
Minor actions required
Significant activity required
Major remediation required.
Self identified in flight / planned actions

REMEDIATION OPTIONS WHEN FUNDING IS NOT AVAILABLE

Firms should also determine whether or not funding has been secured for the remediation plan. Where funding is not secured, there may be other remediation options; for instance an existing change programme/ project may be in place that is addressing or will aid the necessary remediation activity.

Firms should not expect to be able to remediate all vulnerabilities and may have to come to a degree of risk acceptance for some vulnerabilities identified e.g. if the potential issue lies with a critical third party. However, firms should frequently review their risk acceptances and confirm that they are happy to continue accepting them. It is also useful for the regulator to understand areas where firms would breach their impact tolerance.

Area of challenge: how to convey to senior management and regulators that lessons learned have been implemented/there is a remediation in place in the business?

Firms shared that educating NEDs on the operational resilience requirements and gaining their support makes the governance process much easier. It is also important to run education sessions so that they can provide effective oversight and challenge.

Practical approaches to feeding back to senior management and the Board:

- Filter through different artefacts to Board meetings to get them comfortable with all the different elements of the proposals, such as signing off important business services, then at a separate meeting focus on mapping, impact tolerances etc. Having discussed different elements at previous Board meetings, it helps firms build up to a self-assessment.
- Others took the approach of packaging up their important business services individually so that Boards signed off the important business service, associated impact tolerance, mapping of underlying resources and scenario testing conducted at one time.
- Others were taking the approach of sharing everything they had done up to a certain point, bringing a few services each time to board meetings rather than conducting a deep-dive on each artefact each time.

As a result of governance schedules (Boards typically only meet 4 times a year) firms need to allow time to ensure relevant approvals have been sought by underlying committees in addition to the Board.

There are lots of ways to approach Board reporting and it is important that Boards build their knowledge of operational resilience over time to be help them become more informed and to able to provide effective sign-off.

13. LESSONS LEARNED

Firms can look to arrange a debrief session with scenario participants to discuss what went well/what did not go well, scenario response/facilitation lessons learned and what enhancements are needed. Additionally, participants should confirm whether or not in their view, the impact tolerance was set correctly and if the definition of intolerable harm needs to be revisited.

In some cases, such as if intolerable harm materialised faster than planned for, firms may need to review their initial assumptions and feed that back into the impact tolerance definition process. These lessons learned should be fed back into operational resilience functions and be written up in the Self-Assessment document.

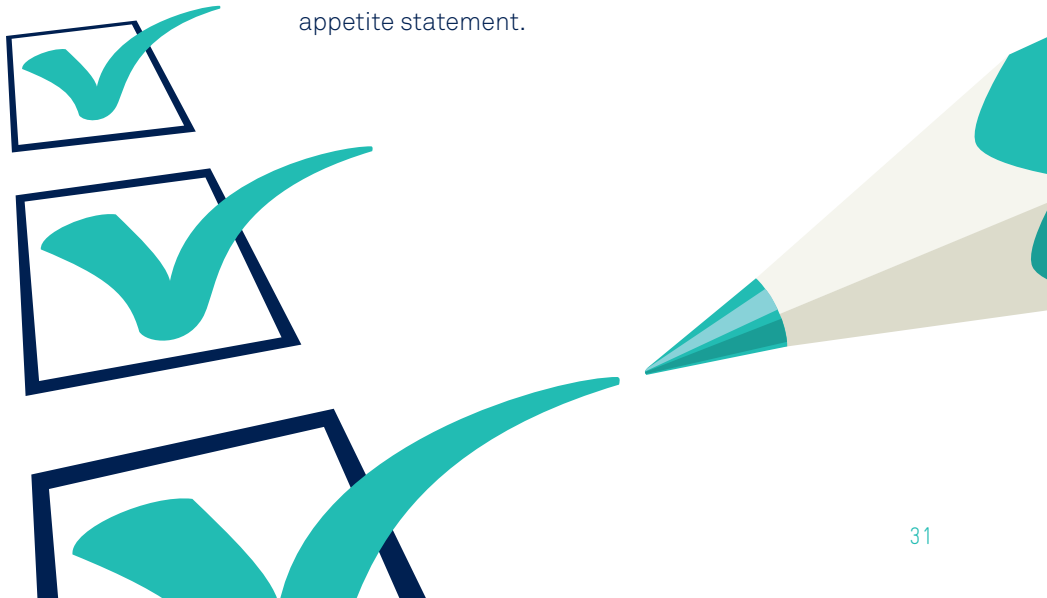
It is important to document all the lessons learned and a summary should be shared with the Board. Some remediation activities may take longer to embed in BAU, but the emphasis should be that firms are learning and actioning these learnings. In the Self-Assessment firms can acknowledge there is room for improvement and that they have a strategic plan in place.

13.1 LESSONS LEARNED CHECKLIST

- ❑ What went well/what did not go well?
- ❑ Was the firm able to remain within their impact tolerance set for that particular important business service?
- ❑ Does the impact tolerance need to be revisited?
- ❑ Were workarounds or substitutes invoked and how effective were these in helping the firm remain within impact tolerances?
- ❑ Does the proposed recovery solution need to be improved in light of the scenario test?
- ❑ Were any vulnerabilities or resilience gaps identified by the scenario test that need to be highlighted to management? Are there solutions already available within the firm to enable recovery within impact tolerance or is investment required to develop a new capability?
- ❑ For a given scenario, what factors could lead to the failure to remain within an impact tolerance?
- ❑ What opportunities are there for improving resilience and further enhancing the firm's ability to remain within tolerance?

Linkages back into operational risk

Where vulnerabilities have been identified, a risk should be raised following the firm's BAU operational risk process. Firms should assess whether any identified vulnerabilities are in line with the firm's risk appetite statement.



14. MATURITY OVER TIME

This paper is intended to provide examples of how firms are approaching testing to determine an approach that suits their individual business model. Firms should recognise that they may be at different stages on the operational resilience journey but that they can expect to build their testing maturity and sophistication over time.

Firms do not need to have performed scenario testing of every important business service by 31 March 2022. However, it is important to have a strategic testing plan in place to articulate how firms plan to meet the requirements over time.

APPENDIX 1

SYSC 15A.5

Testing plan

15A.5.1 R A firm must develop and keep up to date a testing plan that appropriately details how it will gain assurance that it can remain within the impact tolerances for each of its important business services.

15A.5.2 G Firms should ensure that the testing plan takes account of a number of factors, including but not limited to:

(1) the type of scenario testing undertaken. For example, whether it is paper based, simulations or through the use of live-systems;

(2) the scenarios which the firm expects to be able to remain within their impact tolerances and which ones they may not;

(3) the frequency of the testing;

(4) the number of important business services tested;

(5) the availability and integrity of supporting assets;

(6) how the firm would communicate with internal and external stakeholders effectively to reduce the harm caused by operational disruptions.

Testing

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.

15A.5.4 R In carrying out the scenario testing, a firm must identify an appropriate range of adverse circumstances of varying nature, severity and duration relevant to its business and risk profile and consider the risks to the delivery of the firm's important business services in those circumstances.

15A.5.5 G Where a firm relies on a third party for the delivery of its important business services, we would expect the firm to work with the third party to ensure the validity of the firm's scenario testing under SYSC 15A.5.3R. To the extent that the firm relies on the third party to carry out testing of the services provided by the third party to or on behalf of the firm, the firm should ensure the suitability of the methodologies, scenarios and considerations adopted by the third party in carrying out testing. The firm is ultimately responsible for the quality and accuracy of any testing carried out, whether by the firm or by a third party.

15A.5.6 G In carrying out the scenario testing, a firm should, among other things, consider the following scenarios:

(1) corruption, deletion or manipulation of data critical to the delivery of its important business services;

(2) unavailability of facilities or key people;

(3) unavailability of third party services, which are critical to the delivery of its important business services;

(4) disruption to other market participants, where applicable; and

(5) loss or reduced provision of technology underpinning the delivery of important business services.

15A.5.7 R A firm must carry out the scenario testing:

(1) if there is a material change to the firm's business, the important business services identified in accordance with SYSC 15A.2.1R or impact tolerances set in accordance with SYSC 15A.2.5R;

(2) following improvements made by the firm in response to a previous test; and

(3) in any event, on a regular basis.

Lessons learned

15A.5.8 R A firm must, following scenario testing or, in the event of an operational disruption, after such event, conduct a lessons learned exercise that allows the firm to identify weaknesses and take action to improve its ability to effectively respond and recover from future disruptions.

15A.5.9 R Following the lessons learned exercise, a firm must make necessary improvements to address weaknesses identified to ensure that it can remain within its impact tolerances in accordance with SYSC 15A.2.9R.

With thanks to KPMG for their support in facilitating the IA Scenario Testing Working Group.

THE
INVESTMENT
ASSOCIATION

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

www.theia.org
@InvAssoc

December 2021