THE INVESTMENT ASSOCIATION

THE OPERATIONAL RESILIENCE SELF-ASSESSMENT: ARE YOU READY?

January 2022

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

"FIRMS SHOULD COMPILE A SELF-ASSESSMENT DOCUMENT WHICH SHOWS HOW THEY MEET OUR OPERATIONAL RESILIENCE REQUIREMENTS. THE DOCUMENT WILL NOT NEED TO BE SUBMITTED TO US, BUT IT SHOULD BE MADE AVAILABLE ON REQUEST. BOARDS, OR THE FIRM'S MANAGEMENT BODY, SHOULD REVIEW AND APPROVE THE SELF-ASSESSMENT DOCUMENT REGULARLY". – **FCA PS 21/3**

Building a firm's operational resilience is a multi-faceted process, ultimately culminating in the Self-Assessment document. This document forms a key pillar of the firm's operational resilience work and is the main means by which firms will demonstrate to the regulators that they have complied with their rules.

This report represents the output of the IA Self-Assessment Working Group (Working Group), formed to address the requirement for those firms in scope of the operational resilience rules published by the regulator to document their operational resilience arrangements in a Self-Assessment. It also takes into account the discussions held by this group and offers a number of considerations firms can take away and adapt to suit their own particular business models.

Ever since the subject of operational resilience was raised by the UK regulators, the IA has maintained a key focus on this important topic. We established an Operational Resilience Committee and underlying that, a number of task-and-finish working groups made up of operational resilience practitioners amongst our member firms, looking at specific elements of the regulatory requirements. All of these groups have culminated in guidance documents for the benefit of our membership. This Self-Assessment report builds upon our existing set of guidance on Important Business Services, Impact Tolerances, Governance and Scenario Testing, all of which can be accessed on our dedicated expert page: **https://www.theia.org/operational-resilience**.

This report is predominantly concerned with equipping firms to put together their first Self-Assessment ahead of the first regulatory deadline, 31 March 2022. We do include considerations for firms on how they might go about maturing their approach over time, and where necessary, we will consider updating this report to ensure it remains fit for purpose.

Both the FCA and PRA expect firms to summarise the vulnerabilities they have identified to the delivery of their important business services, outline the scenario testing performed and the findings from the tests in a Self-Assessment. However, as the majority of our members are solo-regulated, we focus on the FCA's requirements in particular, although there are a number of considerations outlined that are also applicable to dual-regulated firms as well.

We hope our members find this document useful and insightful as they go about forming their own Self-Assessment documents.

We would like to thank Addleshaw Goddard for their help with facilitating this Working Group and members of the Working Group for sharing their insights.

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

2. PURPOSE OF THE SELF-ASSESSMENT

The purpose of the Self-Assessment document is to demonstrate the firm's resilience journey and how they have achieved compliance with the regulations. Firms will need to document the methodologies used to fulfil the activities set out in the rules, and show the steps they have taken over time to comply with the policy. The Board and senior management have a key role in this process as they hold ultimate responsibility for operational resilience and will need to approve the information provided in the Self-Assessment. The regulators are keen to ensure that Boards in particular understand the impact of disruption. It is an important tool to enable Boards and Non-Executive Directors to discuss what is important, the inherent risks and vulnerabilities identified along with any mitigants and to discuss any investment needed to ensure the firm is effectively able to prevent, recover and respond to disruption.

It is important to note that the Self-Assessment offers a range of benefits to firms beyond mere compliance. It plays a pivotal role in helping the Board and SMF24 (the role-holder(s) designated with responsibility for operational resilience) with the discharge of their responsibilities and offer them comfort on the firm's resilience posture. As the FCA detail, compiling a Self-Assessment document helps firms assure themselves of their own compliance, provide the basis to take necessary action to address weaknesses in their resilience and to provide necessary information for senior management.

MATURITY OVER TIME

The priority for firms in the initial Self-Assessment (period up until 31 March 2022) should be showing their workings, rather than having all the answers. Essentially by 31 March 2022 firms are required to have carried out mapping and testing exercises only to the extent necessary to identify important business services, set impact tolerances and identify vulnerabilities in their operational resilience. Firms can then look to build their operational resilience maturity over the transition period. In particular, as Lyndon Nelson points out in the quote below, firms should focus on identifying their vulnerabilities that would threaten the firm's ability to deliver its important business services within the impact tolerances set.

"The word in the policy documents that is doing a lot of work here is "sophistication" – yes we are asking and expecting firms to have done quite a bit by 31 March 2022, but is it ultimately going to be everything that we expect firms to do? No. We understand and expect that tasks such as mapping and testing will evolve and will grow in sophistication over time. So by 31 March 2022, I would expect that you will be able to set out a ***compelling gap analysis****. You will know where your major shortcomings are and therefore which areas need more work."*
– Lyndon Nelson, Bank of England, Speech May 2021

Prior to March 2022: firms can focus on the design effectiveness of their operational resilience framework, engaging their Boards and senior management in the process.

April 2022 – 2025: firms can focus on embedding their framework throughout the organisation and building their resilience holistically, testing their ability to withstand disruption and mitigate harm. Note that as soon as reasonably practicable after 31 March 2022, and in any event no later than 31 March 2025, firms must remain within impact tolerance for each important business service in the event of a severe but plausible disruption to their operations.

Key considerations to bear in mind:

- **Living document:** the Self-Assessment remains a living document that needs to be regularly reviewed and updated, particularly when there is a significant change to the business. As such, a system needs to be in place to ensure there are regular reviews and approvals for any changes.

- **Proportionality:** the FCA permits firms to apply their operational resilience rules proportionately and in a way which best suits their business, and the Self-Assessment should reflect this proportionality principle.

- **Consumer harm:** firms will need to document how they intend to mitigate harm to consumers in particular, as well as how they intend to minimise risk to market integrity.

- **Justifications and methodologies:** firms should be aware of the emphasis the FCA places on ensuring firms consider their 'justifications' for determining some business services as important and their methodology for setting impact tolerances as well as other key determinations they make. So firms need to show their workings as well as the answers they arrive at. These should be clearly communicated in the Self-Assessment, recognising that it is likely that the justifications and methodologies for firms' resilience arrangements will mature over time. For instance, firms may wish to log all their business services in the first instance, explaining why they identified some as important and discounted others.

- **Vulnerabilities:** the Self-Assessment should be considered an opportunity to communicate and explain the vulnerabilities identified by the firm and any timelines to remediate these. A way of communicating this is via a compelling vulnerability gap analysis. Firms should not expect to be able to stay within impact tolerance for all their important business services by 31 March 2022, but they will need to be able to so by March 2025.

- **Governance:** a firm must ensure that its governing body approves and regularly reviews the Self-Assessment and lessons learned exercise documentation.

- **Enforcement:** the Self-Assessment does have the potential to expose firms to risk if it is not drafted with skill and care. Firms should be mindful of how the document will be perceived in the event that an adverse operational event occurs and harm is caused to consumers. The Self-Assessment will likely be a key exhibit in any FCA investigation or enforcement action. Firms should be aware that as an option of last resort, the FCA has powers under sections 55J and 55L of FSMA on its own initiative to require the firm to take specific steps in line with the FCA's view to comply with their requirements.

There are two golden rules that firms can bear in mind as they draft their Self-Assessments:

- If it is not written down it did not happen
- If it is written down it had better have happened

3. REGULATORY REQUIREMENTS

The Self-Assessment should document the firm's resilience journey and the steps they have taken over time to comply with the policy.

The FCA are very clear on what they expect firms to detail in their Self-Assessment document. This includes:

1. **Important business services** identified and the justification for these
2. **Impact tolerances** set and the justification for these
3. **Mapping** and how this has been used to
   a. identify the people, processes, technology, facilities and information necessary to deliver each of its important business service
   b. identify vulnerabilities
   c. support scenario testing
4. **Testing plan** and justification for this
5. **Scenario testing** carried out, including a description and justification for the scenario design and any identified risks to the firm's ability to meet its impact tolerances
6. **Lessons learned exercise** conducted
7. **Vulnerabilities** identified, remediation actions taken or planned and justifications for their completion time
8. **Communication strategy** and how it will enable the firm to reduce harm caused by operational disruption

Throughout, firms are expected to detail the **methodologies** used to undertake the above activities.

REVIEW PROCESS

The FCA indicate that firms are best placed to decide how regularly this review needs to be performed depending on their business. However, it is the expectation that firms review their important business services and impact tolerances on an annual basis or if there is a material change to their business or the market in which they operate. More frequent reviews of the firm's Self-Assessment document will be required where changes occur that may have a clear impact on the firm's operational resilience, such as structural changes to the firm, rapid expansion, poor trading or entry into new markets. As part of their Self-Assessment process firms may want to think about how to evidence such reviews.

The governance process for the Self-Assessment should be documented appropriately. For instance, firms can consider including a summary of the minutes from SteerCo meetings.

Firms should be aware that the earliest date that the FCA would formally request the completed Self-Assessment document will be no earlier than 31 March 2022. The full detail of firm's Self-Assessment obligations is detailed in SYSC 15A.6 **(Appendix 1)**.

4. FORMAT OF THE SELF-ASSESSMENT

When it comes to determining the appropriate size and format of a firm's Self-Assessment, there is no prescriptive rule. The content and level of detail included within the Self-Assessment should be proportionate to the firm's activities.

FORMAT

The FCA only detail that firms should prepare their Self-Assessment document in a format which is clear and well-structured and that accurately reflects the operational resilience of the firm. As such it is up to firms to choose whether they present their Self-Assessment in the form of a text document, slide-deck, spreadsheet or even a combination of formats if the firm prefers.

Firms can consider including an executive summary, highlighting the key details in the document and in particular to document that the Self-Assessment has been signed off by the firm's Board.

Area of challenge: how can firms keep their Self-Assessments up to date?

Firms should consider what measures they will use to ensure the Self-Assessment document is kept up-to-date and who is going to be responsible for identifying changes to the business that require updates to be made to the Self-Assessment. The Working Group discussed the practical considerations of keeping the document up-to-date. One suggestion is to keep the stable elements of the document within the main section and putting the more changeable elements within annexes which will be easier to update and get signed-off in the future.

SIZE OF DOCUMENT

The document should be as long as needed to accurately represent the size and scale of the organisation. The level of detail should be proportionate to the firm's activities. The Self-Assessment will likely be a large document in order to communicate the complexities of the business and their resilience preparations. Firms can choose to make use of appendices and such alike to convey their justifications for their resilience decisions for instance. The rules also state that the list of what firms should include in their Self-Assessment is 'not limited'. Firms have discretion to include additional information in their Self-Assessment document as they see fit. Firms may wish to include internal or external audit reports, or parts thereof, in the document.

However, an excessively lengthy document can itself be a source of risk and may pose difficulties with getting sufficient NED engagement. Ultimately, the document needs to be the appropriate size and shape for each firm dependent on their size and risk profile.

5. CONTENTS OF SELF-ASSESSMENT

Firms are best placed to decide how they should structure their Self-Assessments. In this section we outline the key areas firms should consider including in their Self-Assessments to ensure they are in full compliance with the rules, taking into account discussions held by the Working Group.

EXECUTIVE SUMMARY

Firms may choose to include an executive summary, pulling out the key details contained within the Self-Assessment. This can include the background of the regulatory requirements and an overview of the steps the firm has taken to achieve compliance.

The PRA has articulated the following strategic outcomes for firms when it comes to building their operational resilience: identifying their important business services, setting impact tolerances and ensuring they are able to remain within these. This could be used as guidance to determine the key aspects firms can include in their executive summary.

In particular, the executive summary can briefly outline the key areas for the Board to sign-off on including:

- The firm's important business services and associated impact tolerances
- The resilience gaps/vulnerabilities identified and any remediation plans in place
- The approval process for the Self-Assessment

Year 1: the executive summary of the Year 1 (March 2021- March 2022) Self-Assessment should address the activities conducted to date and may also detail how the firm intends to build its resilience over the transition period. In Year 1 firms will need to have started to operationalise the policy framework which includes:

- Identifying the firm's important business services
- Setting impact tolerances for each important business service
- Mapping their dependencies and conducted scenario testing to have been able to identify their important business services, set impact tolerances and to identify any vulnerabilities in their operational resilience
- Producing their first Self-Assessment document

FIRM OVERVIEW

It is helpful to set the context of how your organisation is structured, providing an overview of which legal entities in your business are in scope, and those that are not, stating the reasons why. Other considerations for firms to document where relevant include:

- The firm's status within the wider group structure
- Main activities and business lines
- Markets and consumer types served (including a broad assessment of the types of intolerable harm they may encounter)
- Operating model
- Regulatory history
- Client services and internal functions
- Service delivery model
- Scale and nature of key outsourcing arrangements
- Historic incidents

Overview of operational resilience policies and frameworks

It is worth including an overview of how the firm is operationalising the operational resilience rules, including details of the framework in place and how this is being managed.

Additionally, firms can consider including details of their training and competence programmes and how they are building awareness of operational resilience holistically for colleagues, boards and other stakeholders. This can also include whether firms are adopting any recognised standards such as ISO 22301.

Global approaches to operational resilience

Firms may wish to identify whether they are taking global approach to operational resilience and how they are implementing their framework across multiple jurisdictions.

Governance arrangements

It is helpful to outline the firm's governance structure with regard to operational resilience. This can include details of the governance arrangements in place to oversee the operational resilience programme and ensure compliance as well as identifying the key roles and responsibilities. This could include details of the oversight from relevant first, second and third lines of defence, internal audit and other functions.

The firm's approach to record keeping and how the firm will maintain and update the Self-Assessment can also be included. Details of the sign-off process for the Self-Assessment as well as for the important business services and impact tolerances identified are beneficial to include, involving the approvals from relevant Steering Committees and the Board. When including details of approvals, the dates for these should also be clearly documented.

Defining 'sophistication'

The regulators are interested in how firms have designed their operational resilience frameworks. Firms will need to build their level of sophistication over time, and it can be helpful to document their approach towards this. Firms may choose to highlight whether any significant changes are expected in its activities in the period up to 2025. For instance, firms may wish to detail how they expect to develop the sophistication of their mapping and scenario testing.

Building on existing bodies of work

Firms should consider existing operational risk insights gained (for example) from previous incident analysis and current operational risk and data frameworks. This will help ensure that inconsistencies in approach are avoided and efficiencies can be achieved by re-using current work and assessments.

IMPORTANT BUSINESS SERVICES

Firms will need to document their important business services and their justification for how and why they have determined these services as important. Firms may choose to include the full detail of their methodology in an appendix. Firms may choose to include a full, detailed list of all their business services to help justify why some have been identified as important and some not.

After 31 March 2022, firms will be required to review their important business services at least once per year, or whenever there is a material change to their business or the market in which they operate to ensure no emerging vulnerabilities are overlooked.

Area of challenge: should firms document the business services not identified as 'important'?

There is no regulatory requirement to document all the firm's business services. However, given that firms have to justify why some of their business services are important, it might be difficult to make this justification without a broader cohort of business services to refer to. Firms may choose to just give a few examples of the business services not identified as 'important' with a supporting methodology.

More detail on the important business services requirements, practical considerations and other resources are available on our operational resilience expert page.

IMPACT TOLERANCES

Firms are required to set a time-based impact tolerance for each of their important business services, specifying that an important business service should not be disrupted beyond a certain period or point in time. Firms may choose to use a combination of metrics, in addition to a duration metric if appropriate. These impact tolerances will then need to be written up in the Self-Assessment. Firms will also need to document the rationale and metrics used to set their impact tolerances. This should include how they have taken into consideration:

- The point at which intolerable harm occurs to consumers and the point at which disruption could pose a risk to market integrity and to the firm itself.
- How firms have taken into account vulnerable consumers when setting impact tolerances.
- The fluctuations in demand for its important business service at different times of the day and throughout the year to ensure that its impact tolerance reflects these fluctuations and is appropriate in light of the peak demand for the important business service.
- The aggregate harm when multiple business services are disrupted, particularly where they rely on the same underlying system.

It should also be noted that under Principle 11, the FCA expects to be notified of any failure by a firm to meet an impact tolerance. Firms may choose to include the full detail of their approach to setting impact tolerances in an appendix.

More detail on impact tolerance requirements and practical considerations is available in our dedicated paper on this subject Impact Tolerances: Appetite for Disruption.

MAPPING

Firms are required to identify and document the people, processes, technology, facilities and information necessary to deliver each of its important business services. This exercise, known as mapping, must be sufficient to allow the firm to identify vulnerabilities and remedy these as appropriate.

The firm's approach to mapping will also need to be documented in the Self-Assessment including how the firm has used mapping to identify the resources necessary to deliver each of its important business services, identify vulnerabilities and support scenario testing.

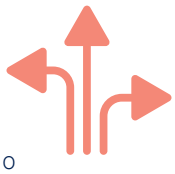
In relation to mapping, firms may wish to document:

- The key sources used to support their mapping
- Where and how mapping is being kept up to date
- How vulnerabilities have been identified
- The key roles that support the delivery of the important business services and the plans in place for individuals fulfilling these key roles being unavailable
- How mapping has been used to inform the design of scenario tests
- Any limitations experienced when conducting mapping in Year 1
- How the firm intends to develop the sophistication of its mapping activities over time

Firms may wish to include the full detail of their mapping in an appendix, including information on the people, facilities, processes, third party providers, technology and information identified that supports the delivery of their important business services.

More detail on mapping business services is available on pages 6-7 of our paper Operational Resilience: Important Business Services.

SCENARIO TESTING



A testing plan and details of any scenario testing that has taken place will need to be included in the Self-Assessment. In Year 1, firms will not need to have tested every important business service, but they are expected to develop the sophistication of their testing over time. Firms may also choose to include any testing that has occurred during the year which contributes to building their overall resilience as opposed to only scenario testing for their important business services.

More detail on scenario testing requirements and practical considerations is available in our dedicated paper on this subject Scenario Testing: Severe but Plausible.

Testing plan

Firms will need to include details of their testing plan and their approach to forming a testing plan. This could include how the plan was designed and approved, the format the scenario testing will take, the proposed scope of testing in Year 1 and how this will develop in sophistication over time.

Other considerations for firms to include in their testing plans:

- The types of testing to be conducted (e.g. whether desktop, simulated or live)
- The scenarios which the firm expects to be able to remain within their impact tolerances and which ones they may not
- The frequency of the testing
- The number of important business services to be tested
- The availability and integrity of supporting assets
- How the firm intends to communicate with internal and external stakeholders to reduce the harm caused by operational disruptions
- The circumstances where remaining within tolerance could cause further detriment e.g. where resuming service could spread a computer virus
- How the firm intends to test both a single important business service and scenarios where multiple business services are disrupted

Firms can also include details on how they have leveraged existing testing that is undertaken such as ICARA stress testing.

Scenario testing

Testing in a range of severe but plausible scenarios is intended to help firms identify areas where further resilience needs to be built. All scenario testing carried out will need to be documented, including a description and justification for the scenario design and any identified risks to the firm's ability to meet its impact tolerances. Firms can include details of any scenario library that they have put together, together with details of the scenario tests that have been performed to date. It is worth noting that the proportionality principle applies here and the FCA indicate that firms should conduct scenario testing according to their size, scale and complexity.

There are a number of areas firms may wish to consider:

- The important business services tested and methodology
- How the scenarios were designed and types of scenario planned
- Key stakeholders involved in scenario tests
- The approach to identifying 'severe but plausible' scenarios (e.g. taking into consideration previous incidents)

A firm will need to carry out scenario testing regularly, following improvements made by the firm in response to a previous test and if there is a material change to the firm. How the firm intends to address this should be communicated in the Self-Assessment.

Testing outcomes

When it comes to documenting testing outcomes, firms should pay particular attention to documenting the key risks and vulnerabilities identified. In addition, firms should include details of any scenarios that saw a breach of impact tolerance and those that did not. This should include an explanation of why the impact tolerance was breached.

Where firms have identified severe but plausible scenarios that would lead to a breach in impact tolerance, it is worth including whether the Board have agreed remediation action is possible or whether they have agreed to a level of risk acceptance. The firm can identify these in the executive summary to clarify what the Board has signed off on.

Testing with material third party providers

Where firms rely on a third party provider for the provision of all or a part of their important business service, firms will need to gain assurance that they can remain within their impact tolerances through severe but plausible scenarios. If a firm is not receiving all the relevant information they need from their suppliers in regard to this, 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, if this was the case, 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. The firm remains responsible for the quality and accuracy of any testing carried out, whether by the firm or by a third party.

LESSONS LEARNED

Lessons learned exercises are a useful means to identify weaknesses and where remediation action needs to be taken. A firm must, following scenario testing or, in the event of an operational disruption, after such event, conduct a lessons learned exercise. If a firm experienced a near miss or live disruption then the learnings from this should also be documented.

Any lessons learned exercises conducted will need to be included in the Self-Assessment. As part of this, firms should describe any lessons that are being implemented to improve their ability to effectively respond and recover from future disruptions e.g. improvements to implementing the operational resilience requirements, third party or technology risk management, reporting and metrics. The focus should be for firms to identify what improvements need to be made as well as where resilience gaps lie and address these to ensure they can remain within their impact tolerances as soon as reasonably practicable but no later than 31 March 2025. Operational resilience is an iterative process, and accordingly the emphasis should be on continuously looking to build and improve firms' operational resilience.

VULNERABILITIES IDENTIFIED AND REMEDIATION PLANNED

Under SYSC 15A.6.1 R firms are required to identify the vulnerabilities that threaten the firm's ability to deliver its important business services within the impact tolerances set, including the actions taken or planned and justifications for their completion time. Any material vulnerabilities identified should be documented within the Self-Assessment.

When documenting their approach to identifying their vulnerabilities, firms can also consider detailing:

- What vulnerabilities have been addressed and how/when
- Which important business services are affected by any vulnerabilities or risks identified
- What vulnerabilities still exist that have not yet been remediated or where boards have agreed to a level of risk acceptance
- Vulnerabilities that might arise from any reliance on outsourced services

Area of challenge: should firms expect to be able to remediate all vulnerabilities?

Every firm will identify its own set of vulnerabilities and it may be possible that some of these will not be possible to remediate in Year 1. It is important to have a proportional approach and firms should document their justifications for the actions they have taken and record when and why it is not reasonably practicable to take a certain measure. In particular, firms can capture proportionality in their decision-making by declaring what they have and have not done and how they intend to mature over time.

Remediation

In addition to identifying weaknesses, firms will need to take action to improve their ability to effectively respond and recover from future disruptions. Firms should have a remediation plan in place with clear ownership and timescales to help them be able to remain within their impact tolerances and document this in their Self-Assessment. This should detail what actions are planned to plug any resilience gaps identified.

When documenting vulnerabilities firms should think about the possible implications necessary remediation will have on their investment plans. For example, if a firm's aging IT system is creating a vulnerability but it is not due an upgrade for another 4 years, they should consider whether they need to bring their investment plan forward, or alternatively, whether the Board is prepared to accept the risk and leave existing plans unaltered. The latter approach may be challenged by a regulator.

COMMUNICATIONS STRATEGY

Firms will need to have a communication strategy and document how it will enable the firm to reduce harm caused by operational disruption in their Self-Assessment.

Some considerations firms may want to bear in mind when detailing their communications strategy for disruptive events include:

- A description of communication channels
- A description of escalation paths, associated roles and responsibilities and identified decision makers
- An overview of internal and external communications plan (taking into consideration how a firm will communicate warnings to consumers and other stakeholders where there is no direct line of communication)
- How and when the communications plan was tested and any associated learnings
- Whether or not the communications strategy was changed as a result of testing
- How firms have considered the needs of vulnerable consumers in their communications strategy
- How they have considered Principle 7 of the FCA handbook: a firm must 'pay due regard to the information needs of its clients' and provide 'clear, timely and relevant communications to stakeholders in the event of operational disruption'. Firms should ensure, in line with Principle 7, that such communications are also 'fair, clear and not misleading'. In the future, firms should be aware of the requirements that will be introduced by the FCA's proposed Consumer Duty which also looks at strengthening communications requirements for retail businesses.

6. KEY CHALLENGES FOR INVESTMENT MANAGEMENT FIRMS

OUTSOURCING

Outsourcing remains a high-risk area and one to which firms should pay particular attention.

Firms should call out in the Self-Assessment document where they rely on outsourcing arrangements identified through the mapping exercise. They can also explain any challenges they are experiencing in relation to outsourcing, along with a plan of how the firm intends to improve upon the situation over time.

Outsourcing delivery of important business services to third party suppliers

Whilst firms may, in whole or in part, outsource the delivery of an important business service, they should note that they cannot outsource their responsibility. Firms need to be prepared for operational disruptions involving material third party providers, regardless of their outsourcing arrangements.

Previous reports in the IA's operational resilience series have emphasised the importance of firms engaging early and working effectively with the suppliers involved in the delivery of their important business services to set impact tolerances and coordinate scenario testing. However, this can be difficult to achieve in practice. Firms can look to adjust contracts as a last resort to facilitate co-testing, for instance, but this too is not always possible. In some circumstances, where practical difficulties prevent the firm being able to comply with the letter of the policy, the fact that the firm has challenged their critical suppliers will show that the firm has not been passive in failing to reach full compliance. In these situations, it would be of benefit to include a supporting narrative in the Self-Assessment document.

Sub-vendors

Monitoring fourth parties is an area of challenge for firms. Generally, firms may be able to gain comfort from any due diligence performed by third party providers on fourth parties. However, third party providers typically have no contractual obligation to provide management information or attestation to their clients.

It should be noted that some third party providers will themselves be caught by the regulations and will have their own operational resilience programmes. In such cases the third party should better understand the purpose of their client's request and should be able to leverage their own operational resilience work to satisfy it.

For the purpose of the operational resilience rules, firms might consider making due-diligence enquiries with their third-party suppliers before 31 March 2022 and document any gaps identified. Firms could then look to build the next level of sophistication by enquiring with service level agreements (SLAs) / fourth-party suppliers in due course.

Intra-group outsourcing

Where firms rely on intra-group outsourcing arrangements these should be called out in the Self-Assessment document.

The FCA and PRA are aligned that firms should not treat intra-group outsourcing arrangements as less risky, and that the requirements and expectations are the same as with fully external outsourcing. However, both also acknowledge that firms may be able to exercise a degree of influence and control over third parties within their group. The PRA Supervisory Statement SS2/21 Outsourcing and third party risk management goes into more specific detail for PRA-regulated firms and provides some scope for proportionality in this regard.

There may be an implicit expectation that intra-group outsourcing arrangements are easier to monitor as they are conducted with affiliates, but this is not always the case. In practice, there are often difficulties with gaining oversight, particularly with entities that reside in other jurisdictions. To help in this regard, firms can consider forming detailed SLAs for each function outsourced to within the group.

The degree of regulatory alignment between the UK and the jurisdiction where the intra-group outsourcing takes place can influence how complicated the process of identifying and effectively managing risks proves to be in practice. For example, both EU and UK firms are expected to comply with the EBA's guidelines on outsourcing, which is helpful to UK firms with intra-group outsourcing arrangements in EU countries. In certain other jurisdictions, however, assessing the risk posed by the outsourced arrangement may be complicated by the absence of common resilience related standards.

DEVELOPING SOPHISTICATION OVER TIME

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.

Building resilience is an iterative process, and firms will be expected to identify areas that they can improve on over time. Regulators will be interested in a firm's workings, methods and plans, and they may question where firms identify no areas to be improved. Accordingly, firms should document their strategic plan to build sophistication in their resource mapping and scenario testing over time.

In practice, this means defining Year 1 and ambition maturity levels for resource mapping to understand where the firm is and where it wishes to work towards. For example, building and improving on the firm's understanding of its resources and dependencies.

For scenario testing, the regulations are not prescriptive on test formats, but firms will need a sound methodology and should be able to evidence that they have a plan in place to be able to increase the level of sophistication of their testing over time.

A key point is that whatever approach is taken, it needs to be documented and justified.

TOOLING

Firms may choose to use a tool to aid them with building their operational resilience as they grow in maturity. Firms should recognise that there is no silver bullet self-assessment tool, but there are a range of options that can help firms manage their data, form business service catalogues, store their scenario library and results of scenario tests.

Firms may wish to leverage existing governance, risk & compliance (GRC) and other operational risk tools, bearing in mind that firms will need to incorporate an important business service lens.

The regulators emphasise that firms should not over rely on tools. It is important that firms take stock of any lessons learned from rolling out their operational resilience strategy before using tooling.

7. GAINING ASSURANCE

There is no requirement for firms to gain assurance over their operational resilience work. However, assurance can provide firms with a level of comfort and validation over the work that has been done. External assurance is not a cure-all, but there is clear value in having an opinion document addressed to the Board that confirms the requirements have been met, good governance is in place and that the decision has been made collectively by the Board. In practice, we observe that individual firms are assessing what level of assurance (including the option to gain no assurance) meets their business needs.

Different types of assurance are available, including:

Generic programme assurance review:
provides high level assurance that the firm meets the regulatory requirements but is likely to be less outcomes focused.

Third line review from an internal audit team:
such a review would focus on ensuring the firm meets the regulatory requirements with a focus on the plan and deliverables in place. This type of review is likely to be done on a co-sourced basis with an external adviser.

Independent external review:
engaging with an external organisation to review whether the regulatory requirements are being met and where any gaps exist. This can be co-sourced with the internal audit team but would have the benefit of being presented as a formal, external opinion.

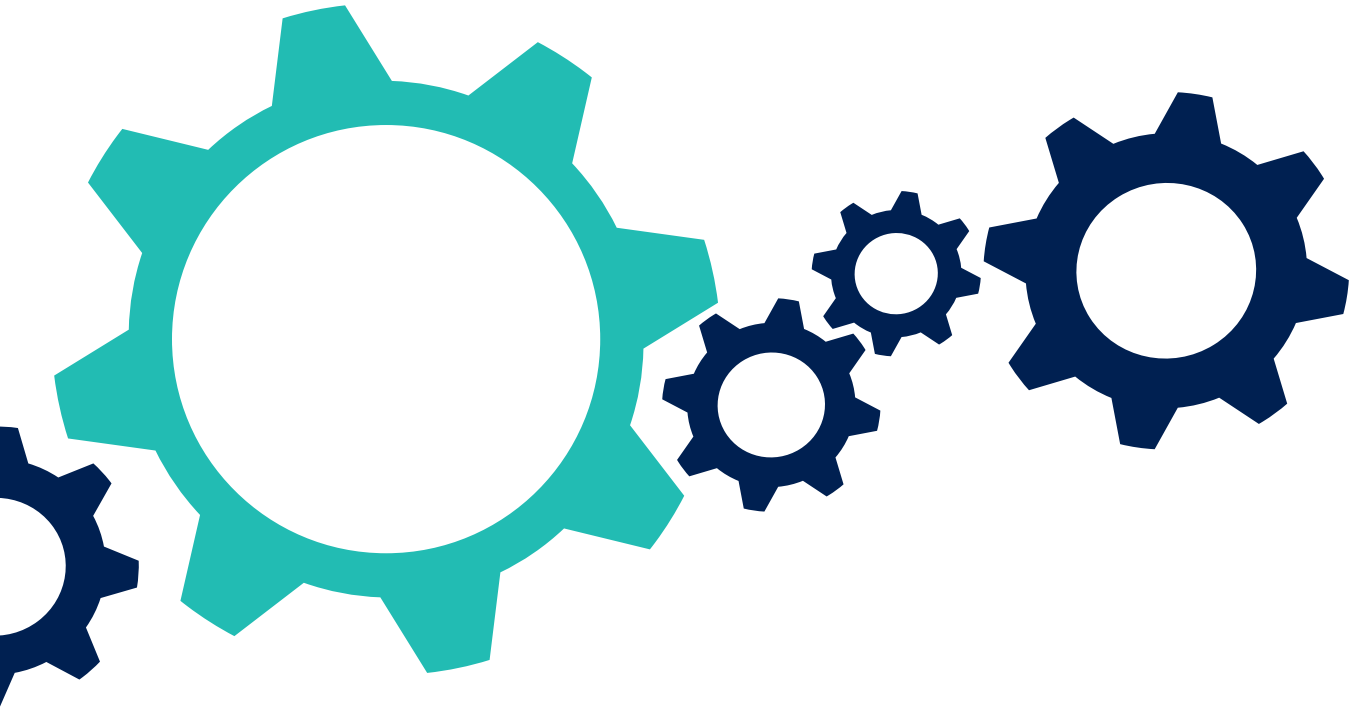
Engaging legal firms:
to gain their view on the legal risks that the firm could be exposed to and how these risks might be managed and mitigated

Firms should consider what actions they will take on the back of such reviews and whether they plan to flag any gaps or embark on any remediation activity before looking for Board sign-off.

8. ONGOING MAINTENANCE & GOVERNANCE

A firm must ensure that its governing body approves and regularly reviews the Self-Assessment and lessons learned exercise documentation. In this regard, the governing body will typically be the firm's Board.

The Self-Assessment is a live document that needs to be regularly updated, particularly when there is a significant change to the business. As such, a system needs to be in place to ensure there are regular reviews and approvals for any changes. Similarly, firms will need to establish an approach to determining what constitutes a material change that would therefore trigger a Board review of the Self-Assessment.



9. CHECK LIST

- ❑ Have all the areas required to be in the Self-Assessment been included? Are the methodologies for all these activities clear?
  - Important business services identified
  - Impact tolerances identified
  - Mapping conducted
  - Scenario testing plan and any testing conducted
  - Lessons learned exercises conducted and details of the findings
  - Vulnerabilities identified and any associated remediation plans
  - Communication strategy
- ❑ Has the firm called out in the Self-Assessment where it relies on outsourcing arrangements identified through the mapping exercise?
- ❑ Have all Board approvals been documented in the Self-Assessment?
- ❑ Has it been documented how the Board will understand and track the outcomes of its Operational Resilience assessment by legal entity?
- ❑ Have the Board's expectations for how it will oversee any significant changes since the last formal approval been documented?
- ❑ Is a system in place to identify potential material changes that would impact the firm's operational resilience that would trigger a review of the Self-Assessment, important business services and associated impact tolerances? For example, structural changes to the firm, rapid expansion, poor trading or entry into new markets.
- ❑ Has the firm's operational resilience governance process been outlined?
- ❑ Has the firm documented its plan for building the sophistication of its resource mapping and scenario testing over time?
- ❑ Has the firm thought about potentially using tools to support the process of developing the firm's sophistication over time?
- ❑ Has the firm thought about whether there is a business need to seek assurance over its operational resilience work?

APPENDIX 1

SYSC 15A.6

Self-assessment and lessons learned exercise documentation

15A.6.1 R A firm must make, and keep up to date, a written record of its assessment of its compliance with the requirements in this chapter, including, but not limited to, a written record of:

(1) important business services identified by the firm and the justification for the determination made;

(2) the firm's impact tolerances and the justification for the level at which they have been set by the firm;

(3) the firm's approach to mapping under SYSC 15A.4.1R, including how the firm has used mapping to:

a. identify the people, processes, technology, facilities and information necessary to deliver each of its important business services;

b. identify vulnerabilities; and

c. support scenario testing;

(4) the firm's testing plan and a justification for the plan adopted;

(5) details of the scenario testing carried out as part of its obligations under SYSC 15A.5, including a description and justification of the assumptions made in relation to scenario design and any identified risks to the firm's ability to meet its impact tolerances;

(6) any lessons learned exercise conducted under SYSC 15A.5.8R;

(7) an identification of the vulnerabilities that threaten the firm's ability to deliver its important business services within the impact tolerances set, including the actions taken or planned and justifications for their completion time;

(8) its communication strategy under SYSC 15A.8.1R and an explanation of how it will enable it to reduce the anticipated harm caused by operational disruptions; and

(9) the methodologies used to undertake the above activities.

15A.6.2 R A firm must retain each version of the records referred to in SYSC 15A.6.1R for at least 6 years and, on request, provide these to the FCA.

Governance

15A.7.1 R A firm must ensure that its governing body approves and regularly reviews the written records required under SYSC 15A.6 (Self-assessment and lessons learned exercise documentation).

With thanks to Addleshaw Goddard for their support in facilitating the IA Self-Assessment Working Group.

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

www.theia.org
@InvAssoc

January 2022