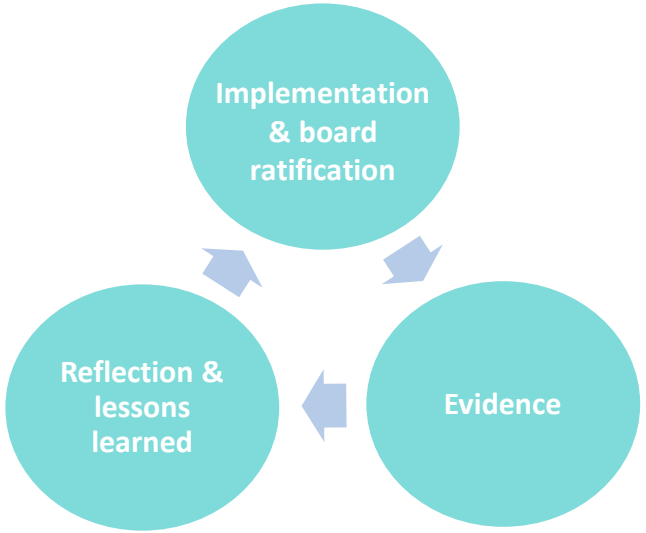
Operational Resilience Self-Assessment Guide

v.1 July 2022

Introduction: What is self-assessment and why is it important?

Achieving the operational resilience requirements and embedding operational resilience into a firm's business is not straightforward. Self-assessment is a vital part of this process, so that firms can evidence *how* they are implementing the requirements *in practice*, enable appropriate board oversight, and demonstrate how their approach to operational resilience evolves over time.



The purpose of the self-assessment process is therefore three-fold:

1. Demonstrate how firms have actually ***implemented*** the requirements in practice and how this supports the overall aim of improving operational resilience. The self-assessment document must provide the information that the board needs in order to ***ratify*** and implement the framework.
2. To document and ***evidence*** this process, the steps that have been taken and the methodologies used. This information needs to be accessible to the board and regulators as required.
3. To provide a living document to help firms ***reflect*** upon their approach to operational resilience as it evolves, including accounting for any changes, vulnerabilities or risks that may emerge, and lessons learned.

For the self-assessment process to be effective, it is important that it does not become a tick-box exercise. It should act as a prompt for what the firm needs to consider and a way to document the steps taken; it is not a substitute for the need for firms to embed operational resilience in their businesses and operations in practice.

What role does the self-assessment document play?

Firms should be able to show that they are learning lessons and learning how to reduce potential for consumer harm. The regulators are looking for operational resilience to secure the safety and security of markets and the reduction of consumer harm.

Without an adequate self-assessment document, it will be difficult for firms to demonstrate how they are actually taking steps to meet the operational resilience requirements, both internally and to regulators. As a result, it is important it is written in a way that is easily understood by an outside party such as an auditor.

Introduction: What are firms required to do?

In-scope firms are required to make and to keep up-to-date a written record of their assessment of compliance with the operational resilience requirements, containing at a minimum the items referenced in SYSC 15A.6.1R. Firms are also required to retain each version of the self-assessment document for at least six years.

Will the FCA expect to see the self-assessment document?

The document does not need to be submitted to the FCA. However, the FCA can ask to see a firm's self-assessment document at any time, for example by requiring a firm to provide a copy or making it available for inspection. Firms are not required to publish their self-assessment documents on their websites.

Having a well structured, clearly thought through self-assessment document ready to provide to the FCA, that clearly explains how the firm has approached operational resilience and embedded this in its processes will also provide a solid basis for any discussions with the FCA.

What does the self-assessment document need to cover?

The self-assessment document must include at least the items specified under SYSC 15A.6.1R. However, the FCA makes clear that this is not an exclusive list; firms can include additional information as they see fit (for example, some firms may wish to include references to internal or external audit reports or parts thereof, post-incident review etc.).

As the business is moving through the transition phase up to 2025 firms should be reviewing their vulnerabilities and carrying out stress tests with evolving complexity. The stress tests should incorporate severe but plausible scenarios and the resulting identified vulnerabilities should then be addressed by the firm in their operational resilience plan.

Self assessments should be regularly refreshed to show the progress made, operating models should evolve and progress in the remediation of vulnerabilities should be documented.

Your self-assessment should look different in 2025.

Why hasn't the FCA or TISA provided an example or template self-assessment document to assist firms?

It's important that each firm's self-assessment document is specific to its own business and their approach to operational resilience. Templates can risk promoting a 'tick-box' exercise. The purpose of this guide is therefore to provide best practice on approach and examples of the sorts of things to be discussed. How firms do so will depend upon the nature of the firm.

However, this guide does provide an example *framework* that might help firms structure the content of their self-assessment. Whichever framework or structure is used, when writing the document, firms should tailor the content to their own specific business, the important business services and the risks/vulnerabilities as they develop over time. The examples in this guide seek to demonstrate how this might be achieved.

Example framework

Note: This is intended as a guide and one example of approach only. Firms should follow the structure and framework that works best for their business and be prepared to justify the approach taken.

STRATEGIC OBJECTIVES		Considerations
A: Set IBS	Justification	Methodologies; Process for review/update
B: Identify impact tolerances	Justification for the level at which they have been set	
C: Remain within impact tolerances	Progress, review and self-evaluation	
SUPPORTING REQUIREMENTS		
Governance, including:	• Governance models, including formal committees, relevant owners and people fulfilling key roles (and plans in case unavailable) • Risks, Issues and Actions, including Key Risk Indicators (KRIs) and relevant governance procedures	
Mapping, including:	• Approach / strategy • Resources identification: the people, processes, technology, facilities and information required to deliver the IBSs • How mapping supports identification of vulnerabilities and scenario testing	Methodologies; Proportionality; Outsourcing
Testing, including:	• Strategy and testing plan, including justification and any assumptions. To include technical review, desktop scenarios, liquidity, capital, third party arrangements, etc. • Description of scenarios used and why • Discuss scenarios where firm could not remain within impact tolerances	
Vulnerabilities, including:	• Discuss vulnerabilities identified • Action plan taken, including justification for completion timeframe	
Lessons learned, including:	• Post-incident review process • Documenting lessons learned, action plan taken, including justification for completion timeframe	
Communication strategy, including:	• Escalation paths • Internal and external communication strategies	

FURTHER INFORMATION / ANNEXES, AS APPROPRIATE

To include further supporting documentation as appropriate for the firm, which might include, for example:

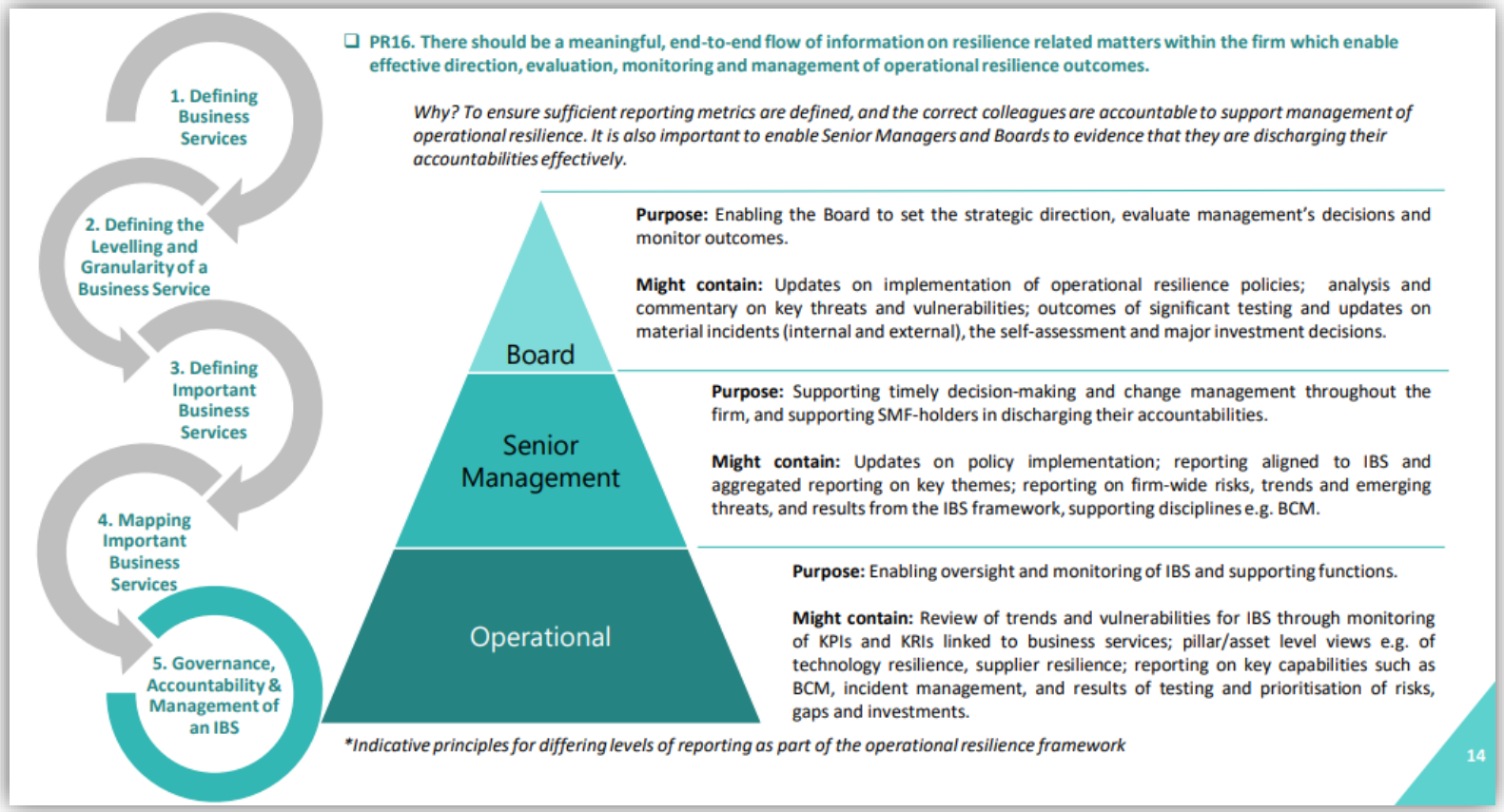
- Change management procedures
- Methodologies: detailed description, data used to monitor performance and embed evidence based practice.
- Key third-party arrangements and dependencies and overview of measures to embed operational resilience, action trackers
- Key personnel and governance arrangements
- Cross-refer to key policies and procedures, and how / when they might need to be reviewed in light of operational resilience objectives

Definitions

	Definition
Self-assessment document	The document that is required to be produced under SYSC 15A.6.1R. It is the primary document through which a firm can demonstrate how they are meeting their operational resilience responsibilities, whether to the board or to the regulator. It should use evidence to demonstrate how that approach evolves over time and is intended to be a living document that is regularly reviewed and updated.
Lessons learned exercises	Following scenario testing or in the event of an operational disruption, the exercise of seeking to identify any weaknesses in order to enable the firm to understand, prioritise and invest in ways to effectively respond and recover from future disruptions. Lessons learned exercises are required under SYSC 15A.5.7R, however this approach should also be encouraged regularly as a firm's approach to operational resilience evolves.
Evidence based practice (EBP)	The approach and method of applying information gathered through research and testing, in order to base decisions and methodologies on objective evidence.

The Board – Self-Assessment review and sign off

This enables the Boards of applicable firms to demonstrate engagement, provide input, oversee and challenge Operational Resilience in their firms. The section below outlines some of the key principles in line with the PS21.3 regulation. It is based on the advice provided under the TISA Important Business Services Guide published in Nov 21 https://www.tisa.uk.com/wp-content/uploads/2022/02/TISA-Important-Business-Services-Guide-November-2021.pdf



- **For the Board to ensure it has sufficient information and oversight of a firms Operational Resilience Self-Assessment it will need to ensure that there is sufficient information provided from both the Operational and Senior Management levels, effectively consolidating all aspects of Operational Resilience under one set of documents.**
- **The next set of slides outlines the key considerations and documents required for an effective Operational Resilience Self-Assessment to be completed.**

Operational Resilience – Board review list

On at least an annual basis, when the Board reviews the self-assessment completed by the business they will need to seek confirmation that the following elements have been completed, or if they have not been that there are adequate mitigation plans in place.

Board Objective: *"Ensuring the firms ability to effectively prevent, adapt, respond to, recover and learn from operational disruptions to its important business services (IBS)."*

Identification & Mapping

Confirmation and rationale for selecting IBSs based on the firms own internal methodology.

Provision and confirmation that mapping has been completed to a sufficient level covering:

- Processes
- Technology
- Third parties
- Information
- Facilities
- People

Baseline Data

Provision of available data for IBSs that quantify the level of intolerable harm caused if disrupted.

For example,

- **Volume** - Numbers and types of clients that use the service,
- **Value** - Financial values and / or impact including analysis for peaks and troughs
- **Period** - Over a representative period relevant to the business (e.g. 5 years)

Impact Tolerance

Rationale and justification from the IBS owners for setting of impact tolerances for each identified IBS assessed for each against the three harms

- **Harm to Client**
- **Harm to Market**
- **Harm to Firm**

This should be based on or informed by the data analysis, if historic data is representative of future events.

Testing

Schedule of Testing activity including output from any completed tests such as lessons learned.

This should include all types of relevant testing such as:

- Technical recovery (IT or disaster recovery)
- Desktop Scenario
- Liquidity and Capital (e.g. Liquidity Stress and ICARA)
- 3rd Party

Governance

As a minimum the Board must have oversight of:

- **Key Risk Indicators** – Data and MI in place to ensure effective management of Operational Resilience at the firm.
- **Risks and Issues** - The identified vulnerabilities identified as part of the process to ensure they have adequate mitigation plans or actions in place.

Communication strategy should underpin all of the above

Operational Resilience – Board review list – Identification & Mapping

For the Board to exercise appropriate and proportionate oversight of a firm's Important Business Services mapping process they need to review and be satisfied with the following:

Identification & Mapping

Confirmation and rationale for selecting IBSs base of the firms own internal methodology.

Provision and confirmation that mapping has been completed to a sufficient level covering:

- Processes
- Technology
- Third parties
- Information
- Facilities
- People

Identification Methodology – A documented methodology for the identification of the firm's important business services, including rationale for selection provided by the IBS owners. This should be reviewed and endorsed by the Board.

Mapping – Oversight of the detailed mapping, including the controls of identified Important Business Services covering the pillars below:

- **Processes** - that are key to the make up the IBS.
- **Technology** – for the above processes to operate
- **Third parties** – required as part of the process (outsource) or supply a key aspect of the IBS (systems).
- **Information** – Information and reports required for processes to operate within the IBS
- **Facilities** – locations/site where key resources operate from, or are required to connect to
- **People** – teams or people resources required to run/ execute processes or steps in the operation of the IBS.

All of the above should be the key aspects required for the operation of the IBS within its agreed impact tolerance

Operational Resilience – Board review list – Baseline Data

For the Board to exercise appropriate and proportionate oversight of a firm's Important Business Services mapping process they need to review and be satisfied with the following

Baseline Data

Provision of available data for IBSs that quantify the level of intolerable harm caused if disrupted.

For example,

- **Volume** - Numbers and types of clients that use the service,
- **Value** - Financial values and / or impact including analysis for peaks and troughs
- **Period** - Over a representative period relevant to the business (e.g. 5 years)

Volume – Detailed analysis of available information of the volume of transactions being executed or processed via the IBS for clients or other end users of the IBS. For example the number of Trades, Payments, Corporate Actions, Transfers In or Out etc. and / or the number of clients placing these instructions.

Value – In line with the above the financial value of transactions being executed or processed via the IBS and its processes. For example the £ value of Trades, Payments, Corporate Actions, Transfers In or Out etc.

Period – Analysis of both the Volume and Value per each identified IBS, over a representative time period. For example trading activity over the past 5 years.

Please note that this is for the firm to determine and should be considered on an IBS by IBS basis. i.e. the representative time frame may be different from one IBS to another.

Operational Resilience – Board review list – Impact Tolerance

For the Board to exercise appropriate and proportionate oversight of a firm's Important Business Services mapping process they need to review and be satisfied with the following

Impact Tolerance

Rationale and justification from the IBS owners for setting of impact tolerances for each identified IBS assessed for each against the three harms

- **Harm to Client**
- **Harm to Market**
- **Harm to Firm**

This should be based on or informed by the data analysis, if historic data is representative of future events.

Harm to Client – For each Important Business Service, detailed rationale and an assessment of the **point** at which intolerable harm occurs for clients of the firm, including consideration of groups of vulnerable clients. This should be expressed as a minimum, either the number of clients impacted or the financial impacts from which they cannot easily recover from.

Harm to Market – As above but for the **point** at which intolerable harm occurs for connected market participants. This should be expressed as a minimum, either the number of clients impacted or the financial impacts from which they cannot easily recover from.

Harm to Firm - As above but for the **point** at which intolerable harm occurs to the firm itself. This should be expressed as a minimum, the financial impacts to the firm to the point at which the Board may consider winding down or implementing recovery action plans to avoid insolvency in line with existing ICAPP/ICARA requirements.

Operational Resilience – Board review list – Testing

For the Board to exercise appropriate and proportionate oversight of a firm's Important Business Services mapping process they need to review and be satisfied with the following

Testing

Schedule of Testing activity including output from any completed tests such as lessons learned.

This should include all types of relevant testing such as:

- Technical recovery (IT or disaster recovery)
- Desktop Scenario
- Liquidity and Capital (e.g. Liquidity Stress and ICARA)
- Third Party

IBS Testing Plan – An annual plan that summarises the scope and breadth of testing activity relating to the firm's important business services, the stakeholders involved and the framework for findings and remediation actions including the timeframes at which the Board will be presented with output. Examples of typical testing activity highlighted below:

- **Technical Recovery** – technical system or infrastructure failover or restore testing usually completed by the IT function to prove systems and functionality
- **Desktop Scenario** – Scenario based 'roleplay testing' with participants simulating an Operational Resilience event and the mitigating action they would take to restore within the agreed impact tolerance
- **Liquidity** – Application and review of the relation between existing regulatory requirements such as Liquidity Stress Testing to the firm Operational Resilience Framework. For example, the point at which a scenario exhausts the firm's liquidity resources should be in sync with the firm harm assessment of any applicable Important Business Service i.e. Dealing, Settlement and Payments
- **Capital** – As for liquidity except that the point at which a Scenario exhausts the firm's capital resources should be in sync with the firm's harm assessment
- **Third Party** – Any of the above with involvement / participation of critical 3rd parties.

Output and Lessons Learned – Agreed format and output from key testing activity for review and oversight by the Board and or delegated Committee or internal Group. This should include the success or failure of the tests themselves, the identified vulnerabilities, risks and issues and agreed action plans.

TISA

Scenario testing and checks

Scenario testing is the testing of a firm's ability to remain within its impact tolerance for each of its important business services (IBS) in the event of a severe disruption of its operations

As per SYSC15A.5 in carrying out scenario testing the 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 firms important business services in those circumstances.

Key checks to be considered:

- Firms are expected to test using a range of severe scenarios and include those where they anticipate exceeding their impact tolerance in order to learn from them
- Firms could consider previous incidents or near misses and lessons learned
- The scenario severity could be varied by increasing the number of resources unavailable for delivering the important business service or extending the period for which a particular resource is unavailable
- Check any scenario that an IBS cannot be delivered within its impact tolerance such as essential infrastructure e.g. power, IT, telecommunications being unavailable
- As part of the transition plan have firms identified the right important business services and impact tolerances based on consumer harm and updated their mapping documentation

During the implementation period (31st March '21 - 31st March '22) firms were not expected to have performed mapping and scenario testing to 'full sophistication'. According to the FCA PS21/3: 'Firms will not need to have performed scenario testing of every IBS by 31 March 2022', but firms will have to have done these by March 2025.

Testing frequency is also relaxed from annual testing to when : 1. there is material change to the business, IBS or impact tolerance set. 2. following improvements made by the firm in response to a previous test. 3. on a regular basis

The regulators will not set industry wide operational scenarios but will consider them as part of their longer term supervisory approach.

Operational Resilience – Board review list – Governance

For the Board to exercise appropriate and proportionate oversight of a firm's Important Business Services mapping process they need to review and be satisfied with the following

Governance

As a minimum the Board must have oversight of:

- **Key Risk Indicators** – Data and MI in place to ensure effective management of Operational Resilience at the firm.
- **Risks and Issues** - The identified vulnerabilities identified as part of the process to ensure they have adequate mitigation plans or actions in place.

Oversight – Review and sign off of the firm's governance model in relation to the oversight of Operational Resilience. This should include the:

- Formal Committee meetings charged with this responsibility and any Working or Steering Groups that operate under it (including Terms of Reference).
- SMF(s) responsible,
- Important Business Service Owners at either an Executive or Operational level or both.

Risks, Issues and Actions – Review of the consolidated log or document capturing all material resilience risks, issues and / or vulnerabilities and their planned mitigation status.

Key Risk Indictors (KRIs) / Early Warning Indicators (EWIs) – The agreed formal governance MI and reporting, including the KRI's and or EWI's that highlight potential issues with the operation of the firm's IBS ahead of material degradation or outage.

These should have appropriate threshold levels and be reviewed periodically or post a material trigger event. For example material incident or testing activity etc.

Communications

As per SYSC15A.8 and PRIN2.1.1R Principle 7, firms must maintain an internal and external communication strategy to act quickly to reduce the anticipated harm caused by operational disruptions. Further, firms should be mindful of the communication needs of vulnerable customers and should consider how they would provide important warnings or advice quickly to consumers and other stakeholders where there is no direct line of communication – see proposed SYSC15A.8.2G. This communication strategy needs to be included in a firm's self assessment document.

There are several areas organisations should ensure they have addressed in developing their communication strategy:

External stakeholder management:

- Customers or clients need prompt and clear information when an incident occurs and during the resolution process. In order to achieve this, firms need to understand their customer or client base, how they engage with the firm, the outcomes that they are looking to achieve, and how these might differ across different customer or client types. This will drive the design of the communication strategy. One size may not necessarily fit all, and firms may want to consider more than one strategy for different customer or client types.
- Whilst customers or clients are clearly a key focus for external communications, firms should also be mindful to consider other external communication that may be necessary, for instance communication with suppliers, shareholders or investors, market infrastructure providers, and the general public. The nature, frequency and format of communications needs to be tailored to these different stakeholder groups.

Regulator engagement: Regulators will expect to be informed on any issues they would reasonably expect to know about. Firms will need to inform regulators on any incident(s) as soon as possible. Organisations should therefore have a clear communication and escalation process in place. Regulators will also expect to see process mapping, tolerance setting and stress testing processes and documents. Identifying current or potential vulnerabilities is essential and again communicating these and how they are being managed to regulators is paramount.

Internal communications: In the event of an incident, or potential near miss, upward information flows should be swift and unimpeded to enable informed and rapid decision making. There should also be a downward dissemination of lessons learned and actions to address.

Firms should be able to utilise existing communication strategies from business continuity and resolution planning work, however these may need to be further fleshed out or enhanced. For instance, firms need to ensure that any existing communication strategy engages important business service owners.

How is Self-Assessment embedded into BAU?

The Self-Assessment becomes a point in time record of the current state of resilience, but it is also a living document that describes the journey and becomes the physical evidence showing year on year how firms are becoming more resilient.

- Resilient by design

This is a loose adaptation of the Data Privacy's principle, "Privacy by design" but it is just as relevant. It describes reviewing new products/ processes holistically and ensuring that each component is resilient; from operations (including supply chain) to the work force that is required to support it to the technology that underpins it.

By ensuring that resilience considerations are made in the initial design phase all the way through to the natural conclusion, means that resilience planning is not an after thought but becomes an integral part of the organisation.

An example of this would be to include resilience requirements as a standard part of the firm's change management and supplier processes, etc.

- Changing the culture of the firm

2 elements that will drive the constructive culture change are:

- Conduct (Behaviours)
- Competence (Skills)

Operational Resilience makes it clear that the Board and accountable SMF(s) are to exercise active oversight of the firms Operational Resilience Framework. Firms should take this opportunity to engage with all relevant stakeholders and ensure they are able to demonstrate that operational resilience is embedded as part of the decision-making process. At high level, considerations should be given to:

- Training requirements for the Board, other senior stakeholders and the frequency of that training
- Understanding of the key recovery controls within the firm's operational resilience capability
- Effective MI and reporting on the operation of the firm's Important Business Services

Operational Resilience Self-Assessment Evidence and Action Tracking

Evidence based practice (EBP) is central to all risk management good practice. When it comes to organisations' operational resilience (OR) and their self-assessment document, the business needs to apply EBP across all the OR regulatory requirements. If applied correctly, EBP will 'bring to life' a firm's OR strategy and ensure all stakeholders including the regulators are aligned in their understanding for how the business is applying, measuring and monitoring their OR progress against the regulations.

When applying EBP, it is wise that a firm's compliance team apply the mantra **'if it is not written down it did not happen**' plus, if you do not have the data, it did not happen! Plus, where the self-assessment document is concerned if it is written down it **had better** have happened.

The fact that the operational resilience self-assessment document needs to be an evidence based living document which is regularly reviewed means that key considerations need to be addressed across:

- **Proportionality:** With the FCA permitting firms to apply their operational resilience rules proportionately which best suits the business. This needs to be evidenced in the self-assessment document and tracked over time.
- **Justifications and methodologies:** Firms need to evidence their decision making in assessing important business services (IBS) and their methodology in setting impact tolerances. These need to be clearly communicated in the self-assessment document and recognising that a firm's justifications and methodologies will change over time.
- **Consumer harm:** Firms need to evidence how they are protecting their customers, particularly any classed as vulnerable.
- **Organisational weaknesses:** Remember the operational resilience regulations test is for failure not success, so it follows that a firm should evidence they have tested for weaknesses and how they can best ensure their IBS remain within their impact tolerances.
- **Governance:** The firm's decision-making bodies and teams must apply EBP and the self-assessment document should evidence research and due diligence particularly for IBS, outsourcing and setting their impact tolerances.
- **Enforcement:** The FCA has powers under sections 55J and 55L of the FSMA to require a firm to take steps to comply with its regulations. This means the self-assessment document will be front and centre for any FCA investigation or enforcement action, so it is imperative the firm ensures EBP is applied throughout the self-assessment document.

Given the self-assessment document is effectively a resolution pack, all the above issues should be addressed and born in mind when a firm designs, deploys and embeds the document into their operational resilience strategy. Action planning and tracking is therefore central to ensuring a firm's self-assessment document addresses all the key regulatory requirements and evidences compliance activities in relation to operational resilience.

Action Tracking Case Study

Designing and embedding an action plan across the operational resilience regulatory requirements, can be a good way to demonstrate you are adhering to your self assessment and resilience journey. Action tracking will also help firms prepare their self-assessment document format, ensuring it is clear, well-structured and accurately reflects the operational resilience of the firm. The action tracking will also determine how often a firm reviews the self-assessment document and relevant regulatory directives. There should be a named person with a specific role to ensure accountability.

SME Retail Investment Advice Case Study and Example Operational Resilience Action Tracking

Risk category	Objective	Risk description	Inherent risk score	Mitigating controls	Residual risk score	Action	Completion date	Person responsible	Target risk rating
Important Business Services	Identified and justified	CRM, Back Office, Dealing Software		Third party MI required		Data requested Against set requirements	01/04/22	Name Role	
Impact Tolerances	Set and justified	Baseline data		Timeline Vulnerable customer information		Vulnerable customer details	01/04/22	Name Role	
Mapping	ID people, processes tech, facilities and information	Organogram In-house and outsourced		Staff turnover, new systems and controls		IBS support roles	01/04/22	Name Role	
Testing plan	Justification	In place		Simulated or live TBC		Frequency	01/09/22	Name Role	
Scenario testing	Description and justification	Previous incidents, testing severity		Impact tolerances set		Design, types, stakeholders	01/11/22	Name Role	
Lessons learned	Exercises conducted	Changes made		Timeline agreed		Exercises conducted	01/02/23	Name Role	
Vulnerabilities	Identified	Remediation		Timeline agreed		What, how, when	01/08/22	Name Role	
Communication strategy	Reduce disruption harm	Clarity, received and understood		Timeline agreed		Channels, escalation paths, roles	01/06/22	Name Role	

Action Tracking Case Study

Action tracking key points
Inherent risk score: Chances of errors across meeting the organisation's objectives
Residual risk: Remaining level of risk following the development and implementation of organisation's response
Target risk rating: Desired optimal level of risk based on ongoing circumstances
Person responsible: Individual(s) and their role(s) with ultimate accountability for risk category, this will vary depending on the size and structure of the firm.