

Operational Resilience Self-Assessments: Trends & Observations Report

September 2024

Authors

Max Cooper

Operational Resilience Manager - Market Governance, Risk and Resilience

Market Oversight and Delivery

max.cooper@lloyds.com

Craig James

Senior Manager, Market Governance, Risk and Resilience

Market Oversight and Delivery

craig.james@lloyds.com

Tel: 0207 327 5078

Paul Brady

Market Oversight Counsel

Market Oversight and Delivery

paul.brady@lloyds.com

Glossary

- **ITols** - Impact Tolerances
- **IBS** - Important Business Services
- **CMORCG** – Cross Market Operational Resilience Collaboration Group

Useful Links

- [The Lloyd's Principle 12 maturity matrix and breach reporting](#)
- [ORCG Guidance November 2023 Guidance for Firm Operational Resilience - TLP Clear - CMORG.pdf](#)
- [LMA Operational Resilience committee documents- including templates, guidance and FAQs](#)
- [PRA Supervisory Statement SS1/21 - Impact Tolerances](#)
- [FCA Policy Statement PS21/3](#)

1 Introduction

1.1 Purpose of this Report

1. Operational Resilience is an “organisation’s ability to anticipate, prevent, adapt, respond to, recover, and learn from internal or external disruption, continuing to provide Important Business Services to customers and clients, and minimise any impact on the wider financial system when, not if, disruption occurs.”
2. The UK regulatory expectation is that in-scope firms will have a fully embedded Operational Resilience framework in place by 31 March 2025. Being able to demonstrate Operational Resilience by design in a firm illustrates the move from ‘project’ to an embedded ‘business as usual’ state.
3. In advance of that deadline, managing agents have produced over the past 3 years an Operational Resilience Self-Assessment the purpose of which is to outline the processes used to comply with the requirements of the regulation. Following the 2022 self-assessment process Lloyd’s issued its first *Operational Resilience Trends Report* (November 2022) designed to offer practical guidance as well as insight into where managing agents were on their regulatory journey.
4. With the UK Operational Resilience transition period ending on 31 March 2025, Lloyd’s has undertaken an updated trends review. This has been based on the latest Operational Resilience self-assessments with a focus on whether managing agents have embedded a sufficient mature and fit-for-purpose robust framework.
5. This report highlights common areas that would benefit from further development and also to provide practical examples of what good looks like as managing agents transition into “business as usual”. As such, anonymised examples of good practice which support further maturity developments are included. We would like to acknowledge with thanks the support of Samatha Nowell and Melody Miller of Sea Change in preparing this report. The contents and findings, however, are solely those of Lloyd’s.

2. Executive Summary

1. We saw good progress in the market's understanding and articulation of Operational Resilience, in particular with the embedding of their "Operation Resilience by Design" frameworks. However, there are some key areas for development which include; clarifying the regulatory definitions and measures of impact tolerances, remediating vulnerabilities and maturing test frameworks to provide a robust answer to the key question; 'can we stay within our impact tolerances?'
2. The themes we saw (and mention below) are also consistent with feedback managing agents reported they had received from the PRA.

2.1 Self-assessments

3. Ten percent of managing agents either did not submit a self-assessment or did not have an up-to-date self-assessment signed off by their board available at the time of Lloyd's request. However, there was a significant improvement in many managing agents' maturity evidenced by well written self-assessment submissions in the majority of the remaining 90%. (Template examples and headers have been shared in this report to assist the self-assessment process.)

2.2 Impact Tolerances

4. Setting impact tolerances (IToIS) is a key part of an effective operational resilience framework. The PRA has requested data in a set format, using the definitions of Policyholder Protection (PP), Intolerable Harm (IH), Firm Safety and Soundness (SS) and Market Financial Stability (FS). However, around half of the managing agents could develop their understanding of the (SS), (PP) and (FS) ITol measure.
5. In addition, some managing agents did not provide enough detail on the rationale or methodology to underpin the ITol time length outcomes in their self-assessment documentation.
6. We also noted that around a third of the market copied values over from different impact tolerance measures without accompanying explanation.

2.3 Testing

7. Testing was the area with the most amount of market variance in terms of maturity and output this year. We were pleased to see good examples where a developed testing framework was being implemented. However, there were instances where no internal testing had been executed, and in some, the self-assessment relied on reporting on the market testing or desktop exercises only, rather than more close-to-live disruption scenarios.
8. Overall, the lack of testing maturity that some managing agents demonstrated was the most concerning element of the self-assessment reviews with some managing agents needing to move quickly to be at an acceptable level of maturity in this area to meet the regulatory requirements. Managing agents must conduct their testing strategy in a way proportionate to their firm's complexity and consider the expected degree of impact of the scenarios chosen.
9. Furthermore, over a third of managing agents did not report testing their crisis communication plans as part of their Operational Resilience scenario test strategy.

2.4 Cycle Review and Triggers

10. To demonstrate a maturing Operational Resilience cycle, firms must discover, analyse, and mitigate vulnerabilities found during their mapping exercises. Remediating these vulnerabilities should be prioritised and delivered as part of the Operational Resilience framework improvement cycle.
11. We found some good examples of this in the market where vulnerabilities identified were prioritised and fed into a change plan to embed and mature the Operational Resilience of that firm. There was found to be a positive correlation between a well thought out plan to address vulnerabilities and the resultant maturity of managing agents' Operational Resilience frameworks. Conversely, where managing agents had not yet highlighted vulnerabilities or integrated them into their plans for mitigation, maturity was rated much lower.
12. The Blueprint Two programme is a key test for the Lloyd's market representing a material change for all managing agents. We were pleased to note the majority of managing agents identified Blueprint Two as an Operational Resilience trigger event. This then informed their future testing plans and was reported in their self-assessments for 2024. Despite the dates of the Blueprint Two cutover moving, the impact and any workarounds were assessed prior to the event to give board assurance. We found that 31% of managing agents did not mention Blueprint Two in their self-assessment, as a trigger or indeed as a testing scenario.
13. It is clear that third party impact will be a key focus in 2025. This means that firms must show third parties are considered sufficiently and included in their Operational Resilience framework, including testing with them where appropriate. Many managing agents did include this as a focus in their self-assessments this year.

2.5 Next Steps

14. Managing agents should carefully consider this report along with the specific feedback Lloyd's will provide to each managing agent. The firm specific feedback and this report should be shared at the managing agent Board or Risk Committee.
15. In some cases managing agents may need to make appropriate remediations to their frameworks in advance of the regulatory deadline. We will continue to engage with those managing agents as we approach the end of the transition period.
16. A consistent theme for many, though not all, managing agents who had not developed their Operational Resilience Frameworks as much as others, was a lack of dedicated resourcing. The development and maintenance of the Operational Resilience Framework represents a significant amount of work. Therefore, managing agents should ensure they are satisfied that the work is resourced and overseen appropriately.
17. Another aspect that some managing agents may need to consider more carefully is the correlation and separation of Business Continuity and Operational Resilience. Operational Resilience is a regulatory requirement with its own terminology and framework. Though firms certainly should look at their existing framework and leverage areas such as risk assessments, DR plans and BCP plans, one is not a substitute for the other. Successful firms aligned materials and utilised existing templates, terminology, and plausibility measures, rather than tried to fit Operational Resilience into existing risk documentation. More mature firms have used Operational Resilience to build a global framework which brings benefits across the business, rather than duplicate work for difference requirements.

3. Trends - Areas Showing Increasing Maturity

3.1 Operational Resilience by Design

Expectations

1. The three-year transition period will end on 31 March 2025 with 'Operational Resilience by design' needing to be embedded by then. This means that managing agents -
 - will be able to stay within their stated impact tolerances from this point, with a robust framework, controls and testing roadmaps in place.
 - will have constructed a Global Framework for Operational Resilience (Building on the UK work completed thus far) – to which jurisdictional changes in regulatory requirements can be built into where applicable for a firm.
 - will have developed roles & responsibility models for timely completion of the actions in their Operational Resilience framework cycle.
 - will have a central change management view for the whole cycle – for example considering internal audit and how monitoring of continuous improvement will take place.
 - will have rolled out board training which should then be refreshed at every major change for the business and when new regulatory policy changes become apparent.
2. Accountability for Operational Resilience also needs to be embedded under the SMF24 function-holder, bringing in responsibility for delivery from appropriate areas of the business, such as Risk Management, CISO, Change Management and Business Continuity. Where there is not an SMF24, firms should have an appropriate senior sponsor for this piece. The board is however ultimately accountable for the framework and relevant policies and procedures.
3. To ensure that the framework is understood and embedded a managing agent may wish to ask:
 - does everyone in the firm know and understand what Operational Resilience is?
 - do they know what the Important Business Services are for their firm and how to report an expected change/impact to them?
 - if anyone in the firm is running activity that could affect an IBS, do they know who triggers their Operational Resilience cycle activity?
 - are all stakeholders confident in what constitutes a 'trigger?'

These are all indicators that Operational Resilience is becoming embedded in the firm.

Review Findings

4. Overall, there was a successful shift towards thinking about Operational Resilience by design, evidenced in the 2025 plans and by pivoting towards BAU in simple and practical ways. A positive example of this is where managing agents built in templates into risk or change functions so that when considering a future change/ project delivery, operational resilience is considered; asking whether the change impacted a resource that supported an IBS/ the IBS itself. Successful managing agents are moving into this pro-active way of considering operational resilience rather than a reactive one, acknowledging the impending deadline and end of the transition period.

5. A key litmus test in this review cycle was the planned Blueprint Two phase I cutover. This represented a material change for all managing agents affecting the most common market IBS. Managing agents that were successful in this area also identified a wide range of triggers in this cycle, prompting them to re-test their impact tolerances and update their self-assessment.
6. Successful managing agents also illustrated a strong governance structure, with clear roles and responsibilities and included demonstrated examples of how Operational Resilience is considered in day-to-day decisions. We saw a clear correlation between firms with an accountable sponsor and governance structure in place and a higher quality of self-assessment and maturity position. However, a third of managing agents' self-assessments gave a limited narrative on how Operational Resilience governance structures are embedded and are operating within the business.

Table a Governance Structure

example of how firms have embedded Operational Resilience through their governance structure; with input from multiple areas of the business into a dedicated Operational Resilience committee working group, that then feed into the overall operational structure and ultimately the board. Everyone across the business is actively participating in Operational Resilience, rather than only the IBS owners.



3.2 Managing Agent’s Self-Assessment

Expectations

7. A firm’s self –assessment ought to be regarded as a self-contained board document which outlines the resilience status of a firm at a particular point in time, as well as the envisaged maturity journey/roadmap ahead. The self-assessment should be updated at least once a year, or when a ‘trigger event’ occurs, giving an accessible view of a firm’s IBS, ITols, testing output and remediation plans. The document in its entirety should answer the question ‘can the firm stay within impact tolerances?’

Review Findings

8. At the time of review, ten percent of managing agents did not have an up to date, board-approved self-assessment available for Lloyd's to review. Of those submitted, there was a broad range of formats, as well as various levels of detail included. Higher performing managing agents demonstrated a consistent assessment in response to all requests from different stakeholders eg into the PRA (in the Regulatory template return), to Lloyd's (under the principle 12 attestation) and to their own Board (in the Self-assessment document).
9. Good examples included self-assessments –
 - that were clear which 'year' the self-assessment document was referring to; showing the firm's current position, the output of this year's cycle and therefore the remediation plans and roadmap to 2025 into BAU and had clear sign off dates and ownership
 - demonstrated three cycles of testing and self-assessment outputs rather than the original 2022 document with certain sections updated
 - included key information within the body of the document rather than links to internal documents, which Lloyd's or a Regulator would not be able to review without additional correspondence
10. We did not see a correlation between a firm's Expected Maturity for Principles Based Oversight and the relative quality of self-assessment; some of the clearest and best-put together submissions were from managing agents expected to be at a Foundational Operational Resilience maturity rating.
11. For managing agents that could benefit from developing their self-assessment format, the Cross Market Operational Resilience Collaboration Group (CMORCG) produced a second iteration of their guidance, laying out a narrative structure that meets regulatory requirements and importantly, makes it clear for a firm's Board to be able to challenge the content, which is also a requirement of the regulation. The CMORCG Self-Assessment guidance was updated in 2023 and [can be found here](#).

Table b Self-Assessment Template

showing header sections./comments to assist firms in how to structure a self-assessment with the above 'narrative' points in mind.

Section title from ORCG Guidance	Additional comments
Executive summary	This should clearly define the narrative of the current year , how the firm has matured since the last self-assessment, with the headlines from the testing output. Can you currently demonstrate you are able to stay within impact tolerances? What are the lessons learnt and remediations ? Were there any changes to the IBSs and ITOLs or any trigger events?
Management of Operational Resilience	Demonstrate how ' operational resilience by design ' is being achieved, how it is embedded in the firm, and how this has matured since the last self assessment
Important Business Services	Confirm they have been reviewed, refreshed , any changes signed off by the board. You may want to have the methodology in an appendix but it should be available
Impact Tolerance statements	Confirm they have been reviewed, refreshed , any changes signed off by the board. You may want to have the methodology in an appendix but it should be available. Include any breakdown of customer types.
Resource Mapping	Clearly outline the resources that support your IBSs . Confirm any maturing or development in this area. You may want to have the methodology in an appendix but it should be available
Scenario Testing	Illustrate the overall testing framework. Outline what testing has been undertaken in this cycle ; how tests are designed, demonstrating that all resource types and all IBSs have been covered. Share testing output- were you able to stay within impact tolerances? For how long? How long was recovery time and what were the workarounds?
Lessons learnt, vulnerabilities and remediations	Output from testing cycle with measurable actions: what are the lessons learnt from this cycle , any actions taken place to remediate vulnerabilities found during testing .
Communication strategy & plans	Outline the operational resilience communication plan and where you have tested it this year
Look Ahead: Roadmap	Include a roadmap into BAU - what areas are you developing in your framework? Testing cycles, actions from the remediations and lessons learnt.

Expectations

12. Cyber resilience is a core part of operational resilience and should be considered when assessing the wider resilience of an organisation.

Review Findings

13. Managing agents that had well established cyber defence capabilities displayed similar features in their attestations such as (but not limited to) -
 - An established and certified (ISO27001) Information Security Management System (ISMS), policies and procedures which are effectively managed and controlled.
 - Good understanding and documentation of Information Assets, Reportable and auditable Security Risk Frameworks,
 - Highly Skilled Information Security Resources, with a high level of staff aware, trained and tested on data protection obligations.
 - Zero Trust security methodologies,
 - Refined cyber vulnerability management process, linked to Operational Resilience as well as Business Continuity Management

3.4 Remediations

Expectations

14. A significant element of both the first year's and subsequent year's self-assessment should be on outlining the gaps, risks and vulnerabilities that have been identified through the work undertaken and the steps the organisation are taking or will be taking to remediate these. This is to allow IBSs to remain within Impact Tolerance by 31 March 2025 and beyond. For situations where firms have identified challenges in respect of remaining within tolerances in the event of SBP scenarios, the Self-Assessment should include the relevant actions which the firm is taking to increase resilience. (CMORCG guidance 2023)
15. To demonstrate a working test framework and embedded Operational Resilience cycle, firms must discover, analyse and mitigate vulnerabilities found during their resource mapping and subsequent internal scenario testing cycles. The Operational Resilience regulation requires firms to:
 - Identify the vulnerabilities that threaten their ability to deliver important business services within impact tolerances.
 - Make every effort to remediate these vulnerabilities, detailing the actions taken or planned and justifications for their completion time.
16. The completion time should be appropriate to the size and complexity of the firm, and the PRA expects large and complex firms to take prompt action. Any resulting vulnerability remediations are to be prioritised and delivered as part of the Operational Resilience framework maturity for all firms.

Review Findings

17. We found some good examples of this in the market where vulnerabilities identified were prioritised and fed into a change plan to embed and mature the Operational Resilience

of these managing agents. This review found a positive correlation between a well thought out plan to address and make progress with addressing known vulnerabilities and the resultant maturity of managing agents' Operational Resilience frameworks. Conversely, where managing agents had not yet highlighted vulnerabilities and integrated them into their plans for mitigation, their maturity was rated much lower.

Table c: Example Remediation and action log

Clearly articulated vulnerabilities, linked to the corresponding IBS supporting resources including prioritisation rationale and plans in place to remediate were evident in some of the best examples in the market.

High Priority – remediated within X weeks
Medium Priority – remediated within X months
Low Priority – remediated within X months

Vulnerability Found	IBS' Affected	Priority	Description	Status	Deadline	Actions
Name of vulnerability 1	Claims Settlement	High	Plan to reach maturity by XX date	In Progress	Jan 2025	X/X complete
Name of vulnerability 2	Underwriting new business, Underwriting MTAs	Medium	Not yet consistently managed through framework	Not Started	March 2025	X/X complete
Name of vulnerability 3	Claims Settlement, Claims Payment	Medium	Not yet consistently managed through framework	Not Started	March 2025	X/X complete

18. However, there were some examples in the market where vulnerabilities had not been identified possibly due to insufficient resource mapping or a lack of sufficient internal testing to date. This would need to be addressed by these organisations to achieve the level of maturity expected of all managing agents by March 2025. An excerpt from the published CMORCG guidance 2023 below sets out some good practice when considering how to document and manage remediating vulnerabilities:

- Detail what actions will be or are being taken to remediate the findings.
- Document who has ownership of the remediation plans and the forecast for their closure.
- For any IBS that has breached Impact Tolerance in a SBP event, define how gaps, risks or vulnerabilities will be remediated and over what timescale up to and past the Operational Resilience transitional period (up to 31 March 2025). This should provide an indication of how long the IBS will be outside risk appetite.
- Remediation activities should be proportionate to the firm and be managed alongside a firm's risk appetite.
- Detail any investment requirements or further investigation for investment to maintain or strengthen the firm's Operational Resilience position. (CMORCG guidance 2023)

4. Trends - Areas Needing Development

4.1 Impact Tolerances

Expectations

1. Setting Impact tolerances (ITols) is a foundational measure for a firm to be compliant and the measure by which firms test they are operationally resilient. Setting ITOLS correctly is vital to enable valid testing. It is important to note that a firm is not able to test sufficiently that they are able to stay within their impact tolerances if they are invalid.

Review Findings

2. All managing agents should have set their impact tolerances by this stage of the transition period and we did not find evidence to the contrary. There was, however, a wide variance as to how managing agents had set their tolerances, the definitions they had used to describe who the impact tolerance was affecting, and how many impact tolerances managing agents had set. This is an area some managing agents should mature their understanding, as we found that over half of the managing agents reviewed showed an insufficient understanding of the below definitions and ITol measures, or not enough detail on the rationale or methodology to underpin the ITol time length outcomes.
3. The regulator has expressed the Impact Tolerance definitions as below in *table d*. ITols are broken down into four definitions, three of which are applicable to the insurance industry. All managing agents completed regulatory returns using the below definitions in the excel template sent in September 2023 (*table e*). Managing agents were correct in understanding that Financial Stability (FS) is out of scope in their self-assessments. This indicates this column should have also not been completed in the regulatory excel return.

Table d: Impact tolerance definitions

Regulator	PRA			FCA
Regulatory definition	Financial Stability (FS)	Firm Safety and Soundness (SS)	Policyholder Protection (PP)	Intolerable Harm (IH)
Where the impact falls	Impact on the Market	Impact on the Firm	Impact on Policyholder	

4. We would expect managing agents to express at least two impact tolerances if they are illustrating them in terms of impact on the Firm and impact on the Customer. Alternatively we would expect managing agents to express three if they are using the regulatory definitions of;

- Firm safety and soundness (SS)
 - Policyholder protection (PP)
 - Intolerable harm (IH)
5. Managing agents should express their impact tolerances under the definitions, rather than the header of 'PRA' 'FCA' without any further explanation. It may well be the case that PP and IH are the same value, as both relate to customers, but it is very unlikely that SS would be the same value as PP and IH. We found that 33% of managing agents had the same impact tolerances values relating to intolerable customer harm to those relating to financial stability (FS), safety and soundness (SS) and policyholder protection (PP) without appropriate rationale. We were also surprised to see some managing agents still only expressing one impact tolerance when considering the above methodology and the regulatory feedback that has been shared thus far.

Table e: snapshot of the regulatory return template sent by the PRA to firms from September 2023. The definitions reflect *table d* above

September 2023 Submission IMPACT TOLERANCES			
(1) Risk of disruption to Financial Stability (Section 1.2 Insurance - Operational Resilience of Solvency II Rulebook) **	(2) Risk of disruption to Safety and Soundness	(3) Risk of disruption to Policyholder Protection (if applicable)	(4) Impact of disruption causing intolerable harm to clients or risk to market integrity

6. The excel template also requested that firms break down their ITOLs to the below values in *table f*, but we noted we rarely saw these measures or level of detail expressed back in firm's self-assessments. More mature managing agents shared consistent data regardless of the audiences as previously mentioned. It is also worth noting that if the analysis has been undertaken to produce the statistics below, it would strengthen the testing framework to utilise this level of detail within the self-assessment itself.

Table f: Itol measures

Length of time (hours)	Point in time	Number of customers	Number of transactions	Value of transactions (£)
------------------------	---------------	---------------------	------------------------	---------------------------

7. Below are examples of where impact tolerances were defined and expressed well. The *Table g* template illustrates a good understanding of the definitions; in how they have considered the firm and policyholder separately for each IBS, as well as considering where the vulnerable customers are, defining separate tolerances where necessary. The Impact on the market is NA, as confirmed by the Regulator and Lloyd's.

Table g: Itol definition workshop template

Impact tolerance	Supporting Stats	Impact on Policyholder	Impact on Firm	Impact on Market	Supporting Rationale
Regulator		FCA & PRA	PRA	PRA	
Definitions covered <i>(Matching the language and definitions in the regulatory request)</i>	Items considered for this column: Where are any vulnerable customers? Which books of business/ entity How many? How many new risks do you write each year, any peak times? How many claims? How many complaints? How many of which are vulnerable customers?	PRA- Policyholder Protection (PP) FCA- Intolerable Harm (IH)	PRA- Firm Safety and Soundness (SS)	PRA- Financial Stability (FS) The impact on the wider financial sector and UK economy	
IBS Name		Questions considered for this column: How long before a consumer (commercial or other) would be adversely affected)	Questions considered for this column: How long before there would be an impact on the firm? At what point would Reputation damage, loss of business occur? What could the business tolerate.	NA	
IBS Name				NA	
IBS Name				NA	
IBS Name				NA	
IBS Name				NA	

Table h: Itols set in a global structure - example of expressing impact tolerances in a global framework. Many firms will have other regulators to consider under the 'Operational Resilience' banner and being able to pull them together creates a robust and effective framework, rather than a duplication of work. The below example seeks to define the impact tolerances by 'prudential' and 'conduct authority' with the correct understanding of these areas defined using regulatory language.

IBS Name	Impact Tolerances								
	1 DAY	2 DAY	4 DAY	7 DAY	14 DAY	30 DAY	2 MONTH	3 MONTH	4 MONTH
IBS 1	MAS, CBI FCA PRA			MAS, CBI FCA PRA			CBI PRA		
IBS 2									
IBS 3						FCA PRA			
IBS 4				MAS, CBI					
IBS 5		MAS, CBI FCA PRA							
IBS 6									

Key

- Conduct Risk** – (IH) (PP) - Risk of serious customer detriment or loss of policyholder protection
- Prudential Risk** – (FS) - Risk to financial safety and soundness of the firm; e.g. reputational or financial damage
- Both** – (FS) (IH) (PP) - Risk of disruption of financial safety and soundness of the firm

4.2 Testing Maturity

Expectations

8. To meet the March 2025 deadline, firms must be able to demonstrate they are able to stay within their impact tolerances for their Important Business services. Firms should have performed at least one cycle of robust testing; making the testing framework and output the backbone of the self-assessment.

9. The expected focus in a self-assessment is ‘what are the impact tolerances for our IBSs and have we proved our ability to stay within those tolerances? What are the remediation plans for vulnerability areas we have found?’ A comprehensive set of tests will answer these questions.

Review Findings

10. Most managing agents have developed a scenario library of severe but plausible scenarios and performed some internal testing during the transition period; translating findings into remediation plans and roadmaps for future testing. Managing agents have clearly engaged with material from the LMA, ORCG and Lloyd’s to achieve this, so there is evidence of some consistency. The majority also leveraged market testing and included the findings in their self-assessment.
11. However, we found testing was an area for development for the market in terms of maturity overall. There was a wide variance in testing maturity and testing types, with many managing agents only having performed or planning to perform desktop tests. The regulatory expectation is that firms will have plans to perform more mature testing as the transition period ends.
12. *Table i* below gives other examples of testing types beyond desktop testing for firms to consider in their testing roadmaps.

Table i: Testing types

Test Type	Characteristics
Penetration Testing	<ul style="list-style-type: none"> • Often performed by a third-party supplier • Can be 'no notice' or planned scenarios. • Controlled measures
Simulation / War Game	<ul style="list-style-type: none"> • Designed to depict an actual or assumed real-life situation • Competitive / contested environment • Use of technology / techniques to engage participants and create stress • Provides an opportunity to rehearse the steps and timeline for response and recovery in as close to real life as possible.
Stressed Exit tests for key suppliers	<ul style="list-style-type: none"> • Practices an exit from a key supplier. • Exercises how to put backups in place rather than theoretically; how to switch over, how seamlessly this can be performed and how long it takes. • Supports Third Party resource pillar
Live Systems or Operational Testing	<ul style="list-style-type: none"> • Real time • Test / Production • Recovery environment • Provides data on timeline of restoration of IT infrastructure, systems, and applications. Identifies any issues in recovery and rehearses supporting plans. • Provides data on ability to recover to Work Area Recovery sites / similar.

13. We also found a third of managing agents defined the testing output as pass/fail rather than measurable output, or asking questions such as ‘how long could we stay within impact tolerance for?’ ‘How long was recovery time?’ This informs the remediation plan. 31% of firm did not present testing output that was connected to remediation plans or showed a firm’s current position.

14. The regulator has confirmed that firms can use the shorter of their impact tolerances when testing, but this does not mean you are only testing one impact tolerance. For example, if you are using 30 days as the impact to customer ITOL, but the impact to the Firm was 60 days, your testing output should still consider how the scenario affects both parties, as there will be different work-arounds and effects during a test. We also noted

22% of managing agents did not have a test plan included in the self-assessment document or demonstrated plans going up to October 24 rather than 2025.

15. To assist the market in this area, we have firstly shared an illustrative testing framework in *table j* below, which takes key elements to design and execute a series of tests from a developed scenario library. It demonstrates how the output of testing should be formalized into a remediation plan and form the basis of a firm's self-assessment each year.

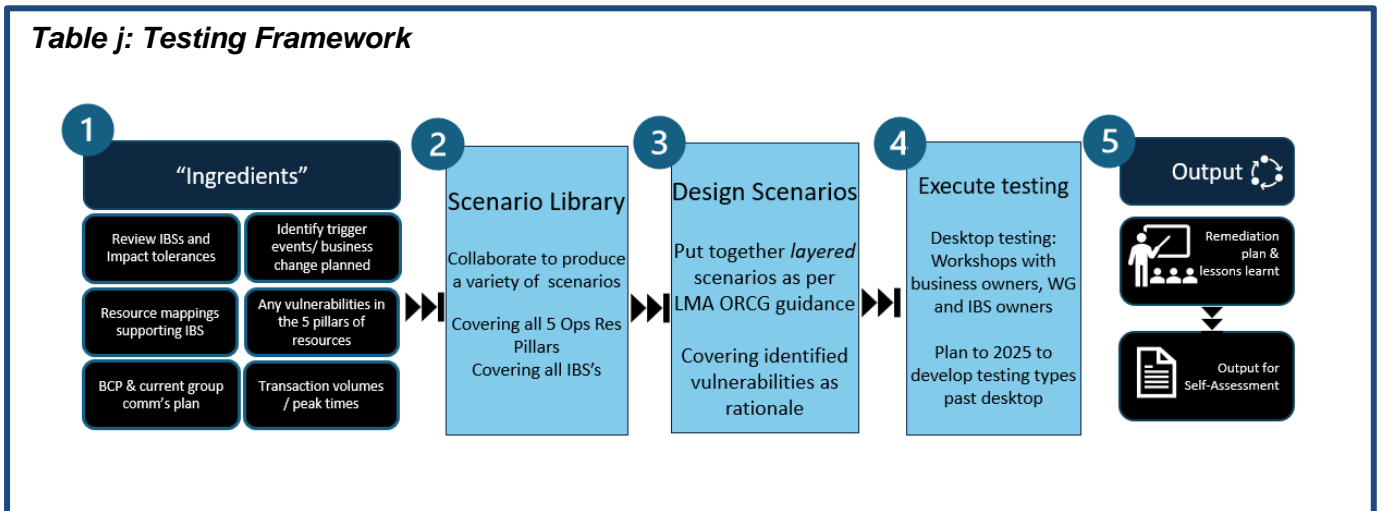


Table k sample testing output format example- reflecting how a firm can successfully demonstrate the status of an IBS through testing its impact tolerances. The below example also shared the findings of the testing specific to the IBS, lessons learnt, vulnerabilities and how this then fed into the firm's remediation plans. You can see the firm's current position through all its IBS and included all the information needed to review the firm's position.

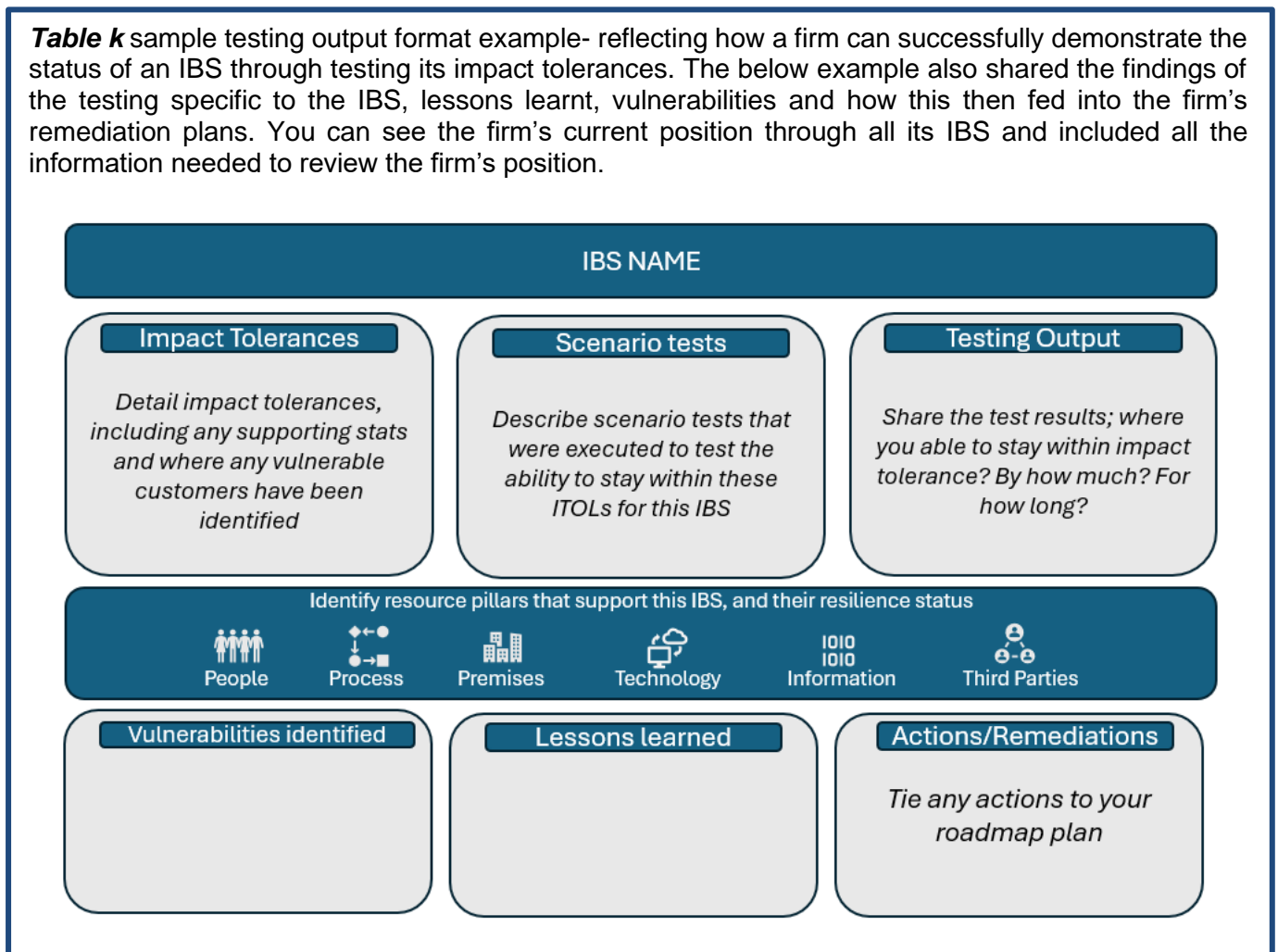


Table 1: Scenario output demonstrates an example guidance of running a scenario test and the types of considerations firms may need to take into account to ensure the right breadth of scope is included when assessing whether they can stay within their impact tolerances following more mature testing such as a Structured Scenario Exercise (SSE), Simulation, War Game, Live system or Operational Test.

	Key elements of response and recovery	Rationale	Comments	Vulnerabilities/Lessons learned from this stage
1	Failure/disruption is assumed	Ensure participants are aware not to challenge the scenario, firms are dealing with inevitability. Testing should focus on detection, containment, mitigation, response, and recovery actions.		
2	The invocation of the Impact Tolerance(s) should be recorded from a time stamp perspective.	This is to ensure that operational disruption being tested is tracked against the scenario and ultimately if the Impact Tolerances were breached or met.		
3	As duration of recovery is important to assessing the outcome, testing should consider activities that impact the timeline	This should include things like the time required for data analysis during an incident, decision making etc. Previous testing and incidents can be leveraged.		
4	Setting out how the disruption will be detected and what controls or processes that firms will be reliant on so that appropriate response and escalation will be triggered.	Include indicative timeline based on experience / known incidents? How would this differ during a disruption to 3rd party / FMI?		
5	What are the immediate response steps that would be taken?	In some circumstances taking the systems and therefore the business service off-line might be the safest and most effective immediate response to the event		
6	What are the communication requirements (internal and external audiences) for the scenario envisioned,	This should include who would provide updates to crisis structures		
7	Containment actions: where relevant, what actions will firms take to contain or limit the amplification of the impact, within the organisation and external to other customers, third parties or FMIs.	For example, factors that may lead a firm to take action to disconnect from a third party and FMI or customers to its systems. What are the post-incident service recovery actions including reconnection criteria.		

Table I: Scenario output (contd..)

	Key elements of response and recovery	Rationale	Comments	Vulnerabilities/Lessons learned from this stage
8	Articulating the impact,	leveraging defined Impact Tolerance metrics to enable targeted response and mitigating actions.		
9	How effective are mitigating actions in reducing impact / harm to consumers, the firm, and the wider sector?	Is there a solution that might mitigate impact for some of the impacted consumers, even if not all? How sustainable are these mitigations, and will they extend the point at which intolerable harm would be breached? Are there options for a partial resumption of service (manual payments for example), or the delivery of an alternative service, which would mitigate impact? Are there alternative channels that can be used, and do they have the capacity to handle increased volume? How effective are third party mitigations?		
10	Are the mitigations in place effective for all harm factors e.g., consumer, market integrity, safety and soundness, and financial stability (where applicable)	e.g., a mitigation for consumer harm may not be effective to mitigate risks to financial stability?		
11	What relevant response and recovery plans and playbooks are in place, a	How long does the recovery take? Which activities can be completed in parallel and where are there hard dependencies?		
12	Who will support the response and recovery?	CISO, operations, claims, and how the Resource profile might change over time.		
13	For data- related scenarios	What is the data recovery strategy, including effective execution of data reconciliation to ensure data integrity so that services can be resumed safely?		
14	Additional Impact Tolerance Metrics	In addition to the time metric, has the test demonstrated that the threshold of harm to customers, and the firm have not been breached?		
15	Point of Intolerable Harm	Does the test confirm the assumptions made in the Impact Tolerance statement (e.g., the point at which intolerable harm would occur), or could intolerable harm materialise more quickly or slowly than expected?		

4.3 Change Triggers

Expectations

17. In addition to the minimum annual review, it is crucial that managing agents review their important business services following significant change and as such should be aware of the kinds of changes that would require a review.

18. Triggers could include, but are not limited to;

- Implementing new software,
- Mergers or an acquisition,
- Migrating to the cloud,
- Outsourcing, or insourcing a service supporting an IBS,
- Material adjustment to a Third-Party service supplying or supporting an IBS,
- Any other planned material change that would affect the key resources (people, processes, facilities, data, technology) that support the IBS.

Review Findings

19. Managing agents that were successful in this area were able to recognise the relevant operational change triggers expected for their organisations within this cycle and were prompted to re-test their impact tolerances and update their self-assessment in response to them. However, 46% of managing agents mentioned no triggers expected or occurring at all in this cycle and so we recommend managing agents should review and consider the advice and categories from the regulator below.
20. A key litmus test for the market in 2024 was the planned Blueprint Two phase I cutover. This change affects all Managing agents in the Lloyd's market. Some managing agents planned testing scenarios and workarounds to stay within impact tolerance should the phase I cutover fail for any length of time. This level of maturity demonstrates the foresight that an embedded framework should provide for all managing agents. We found that 31% of managing agents did not mention Blueprint Two in their self-assessment, as a trigger or indeed as a testing scenario.

5. Third Parties

Expectations

21. The PRA expects firms to be able to remain within impact tolerances for important business services, irrespective of whether they use third parties in the delivery of these services. This means that firms should effectively manage their use of third parties to ensure they can meet the required standard of Operational Resilience. Although firms may assume that an arrangement is inherently less risky where the service provider is part of its own group, this may not be the case. The PRA expects firms to manage risk and make appropriate arrangements to be able to remain within impact tolerance, whether using third parties that are other entities within their group or external providers.
22. All managing agents are required to carry out the following activity in relation to Third Parties:
- Identify all third parties, connected sub outsourcing arrangements and intra group arrangements which support the delivery of an IBS.
 - Ensure all material third parties are operationally resilient - if a third-party provider supplying an IBS fails to remain within impact tolerances, that failure is the firm's responsibility.
23. Third party dependencies with regard to a firm's Operational Resilience will be a key area of focus for the regulator in 2025. This means that firms must understand which third parties are considered material to their identified IBS and that testing of those third-party resources supporting these IBS are sufficiently tested. If deemed necessary after testing then suitable workarounds or alternatives need to be available or in place to ensure that in the event of severe disruption, a firm can stay within its documented impact tolerance levels.

Review Findings

24. Many managing agents did include this as a focus in their self-assessments this year, however some did not show any evidence of considering this within their self-assessment documents, which is an area of concern.
25. Every firm's supplier and IBS footprint will be unique, so a mature test framework including testing with material third parties is important for firms to achieve the desired maturity expected in the regulation.

26. Understanding your reliance and dependency on Third Party supply chain, identifying any vulnerabilities including developing alternatives and manual workarounds are crucial steps to ensure your managing agent can remain resilient during severe but plausible events.

4.5 Communications Plan

Expectations

27. All firms should have developed a crisis communication strategy and plan to execute this within the business. This should include reporting to the various authorities/regulatory bodies, such as Lloyd's, PRA and FCA.

28. The PRA expects firms to develop communication strategies for both internal and external stakeholders as part of their planning for responding to operational disruptions. These communication plans should be developed with a view to reducing harm to counterparties and other market participants and supporting confidence in both the firm and financial sector. This should also include the escalation paths to manage communications during an incident and to identify the appropriate decision makers. For example, the plan should address how to contact key individuals, operational staff suppliers, and the appropriate regulators.

Review Findings

29. Over a third of managing agents did not report testing their crisis communication plans as part of their Operational Resilience scenario test strategy. Some communication plans were non-existent or not described in sufficient detail within managing agents' self-assessment. There were, however, some good examples of considering how communications fits within a successful and mature test strategy found in the Lloyd's review.

Table m: Communication Strategy template below lays out an example structure of what to include and how to tie this to operational resilience.



- Detail the firm's overall **communication strategy**
- Describe how the communication strategy helps reduce disruption during an incident i.e. **how it fits in to the operational resilience structure**



- Outline the communication plan during a disruptive event **as tested in scenarios**
- Outline **when the communication plan was last tested and by who**
- Detail any **lessons learnt**
- **Detail any changes as a result** to the plan, roles, or messaging

Disclaimer

Whilst all care has been taken to ensure the accuracy of the information in this document, Lloyd's does not accept any responsibility for any errors or omissions. Lloyd's does not accept any responsibility or liability for any loss to any person acting or refraining from action as the result of, but not limited to, any statement, fact, figure, expression of opinion or belief contained in this paper.

Our Report only comments on significant matters that were identified during the Review, together with any other related matters that we wish to bring to your attention. It is in the nature of this Review that only certain aspects of managing agents' operations are examined within a particular timeframe and at a certain level of detail. Shortcomings may therefore exist which were not identified during the Review. Whilst managing agents may have provided Lloyd's with various items of documentation to enable the Review, by necessity our Review was strictly limited in scope. The absence of feedback on a particular item either within or outside of the scope does not therefore imply tacit approval of the approach set out therein. Where we may have identified issues outside of our scope, we will endeavour to take them forward with managing agents outside of the scope of this review, though that may occur as part of other Lloyd's oversight activities.

To note: All artefacts used within this document have been adapted from examples as part of the review and are to be regarded as good practice examples only rather than treated as a prescribed requirement.