LLOYD'S

Operational Resilience: Lloyd's Market Trends & Observation Report

September 2026

Contents

1. Introduction and Purpose

As the world's leading marketplace for insurance and reinsurance, Lloyd's plays a crucial role in enabling businesses, communities and economies to recover from adversity. In an increasingly interconnected and uncertain world, operational disruption is an inevitable reality. Geopolitical instability, cyber threats, technological advancements, third-party failures, climate-related events and other emerging risks continue to test the resilience of firms across the insurance market.

A resilient market is one that can continue to deliver critical services and recover effectively when disruption occurs, preserving confidence and ensuring those who rely on Lloyd's can continue to access the protection and cover they need. In response to demand from Managing Agents for practical best-practice guidance and aligned to Lloyd's 'Advance and Protect' objectives, this report provides an opportunity to reflect market-wide experience, peer benchmarking and collective learning back to participants and support continued improvement across the market.

As per the Lloyd's Principles Based Oversight framework approach, Lloyd's undertook oversight activity of a subset of self-assessments this year, with the statistics and examples presented drawn from this subset. By sharing key themes, trends and resilience practices, Lloyd's aims to support the maturity of individual Managing Agents and strengthen the stability and long-term resilience of the market.

2. Executive Summary

The 2026 review shows a market that has moved beyond initial regulatory implementation and is increasingly embedding Operational Resilience as a business-as-usual capability. Frameworks are more mature, governance is clearer, impact tolerances are better understood and firms are undertaking more testing.

As the market continues to mature, the key message for 2026 is that maturity is now judged less by whether frameworks exist, and more by whether they demonstrate resilience outcomes in practice.

Material observations:

Testing activity has increased, but outputs need to mature to demonstrate real recoverability.

Managing Agents are undertaking more testing, with an average of 6 scenario tests per year and 80% having tested all Important Business Services (IBSs). However, most testing outputs continue to rely on pass/fail conclusions or assumed recovery timelines. Going forward, successful testing will require firms to evidence not only that testing has taken place, but also the end-to-end recovery timeline, the capacity and sustainability of workarounds, the process for returning to Business as Usual (BAU), and how lessons learned have been translated into remediation or operational change.

Third-party resilience activity is increasing, but dependency risk remains material.

Third-party testing increased by 30% year on year, with around 60% of the reviewed population testing third-party scenarios in 2025/2026. This is positive progress, but the market remains exposed where providers support multiple firms and operational dependencies are concentrated. We have already seen strong examples of shared testing and learning across the market, creating a clear opportunity to further strengthen collective resilience through joint testing, provided all firms contribute in a proportionate manner.

> “The key message for 2026 is that maturity is now judged less by whether frameworks exist, and more by whether they demonstrate resilient outcomes in practice.”

Impact tolerances are well understood with opportunity for further calibration of sub-tolerances.

Firms generally provided clearer rationale for IBSs and Impact Tolerances (ITols), with evidence of tightening in Safety and Soundness tolerances across Claims, Underwriting and Complaints. More mature firms are beginning to use sub-ITols and supporting measures, but these are not yet consistently reflected in testing output. A key next step in the maturity journey is for firms to support impact tolerance rationales with relevant volumes, metrics and sub-measures that can then be used to design and evidence testing.

Emerging and interconnected risks require a more dynamic approach.

Cyber, Artificial Intelligence, cloud and data, geopolitical, people and third-party risks are increasingly connected. Horizon scanning is improving, but firms do not always translate those insights into actionable resilience output such as refreshed vulnerabilities, scenario tests or remediation activity. A key resilience success factor will be the ability to translate horizon scanning and threat intelligence into rapid testing and remediation so as to have a tangible effect on resilience outcomes.

Cyber recovery is now a key differentiator.

Cyber risk continues to evolve in speed, scale and sophistication, and remains one of the most critical and potentially destructive incident types facing the market. Most Managing Agents have strengthened their cyber controls and recovery capabilities for severe but plausible cyber events. The differentiator will continue to be whether firms can demonstrate that following a severe cyber event, they can restore the services that matter most to customers and the market within agreed tolerances, supported by clear priorities, decision-making and recovery plans. This requires continued uplift in recovery capability, Board-level awareness of the residual risk, and clear evidence that cyber recovery assumptions have been tested against increasingly more plausible destructive scenarios.

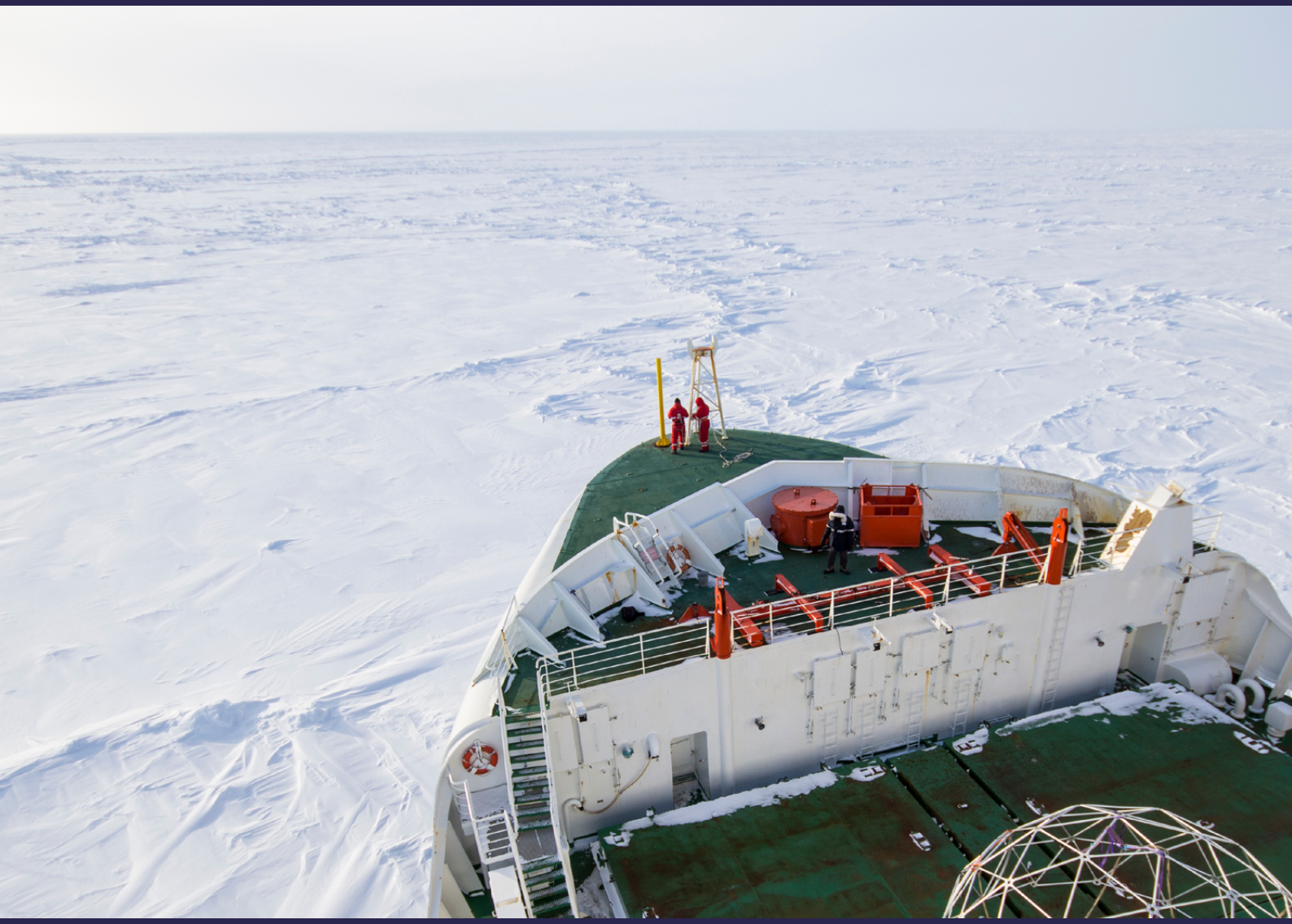
People resilience remains a strategic priority.

Managing Agents consistently recognise that specialist expertise, leadership judgement and operational knowledge are critical to the delivery of IBSs. However, testing still often assumes that people will continue to operate effectively through prolonged disruption. Going forward, firms should assess how sustained pressure, reduced capacity, fatigue and competing crisis priorities could affect decision-making, service delivery and recovery. The strongest firms will treat people resilience as a core component of operational resilience, ensuring that workforce planning, succession, training, wellbeing and crisis leadership arrangements are robust enough to support critical services during extended disruption.

3. Next Steps

We encourage Managing Agents to carefully consider this report along with any specific feedback Lloyd's provided in their oversight cycle. The Managing Agent specific feedback and this report should be shared at the Managing Agent Board or Risk Committee.

Managing Agents can continue to focus on embedding Operational Resilience with an increased emphasis on outcomes and remediation activity. This includes strengthening Board engagement and evolving testing output to better understand real-world vulnerabilities, including the impact of prolonged stress on people and leadership decision-making. Ultimately, operational resilience maturity will be determined not by how effectively frameworks are documented, but by how successfully lessons learned are translated into tangible actions that enhance a firm's ability to prevent, withstand, respond to, and recover from future disruption.



4. Trends – Areas Showing Increasing Maturity

4.1 Moving from Design to Resilience in Practice

4.1.1 Context

With the transition period for SS1/21 concluding on 31 March 2025, the regulatory expectation is that Operational Resilience is no longer viewed as a programme of implementation but as an embedded business capability. 'Operational Resilience by design' refers to the embedding of resilience considerations into business strategy, governance, change management, technology transformation, outsourcing decisions and day-to-day operations.

The Bank of England's Insurance Supervision 2026 priorities reinforce this direction: Operational Resilience remains a core cross-sector supervisory priority, and firms are expected to demonstrate that resilience is embedded in how they operate, change and recover.

4.1.2 Observations

A clear theme emerging from this years' self-assessments is increased evidence that Operational Resilience frameworks are well embedded.

Most firms are no longer describing Operational Resilience as a standalone programme, project or regulatory change initiative; rather, it is increasingly presented as a core business capability that is embedded within their day-to-day operations, governance and risk management processes.

There is growing evidence that resilience is being considered "by design" in change management and business decision-making including in areas such as:

- New project requests such as IT transformation or modernisation
- Resource and succession planning
- Third party assurance and on-boarding

IT change remains a significant driver of Operational Resilience risk. Despite legacy technology making up just 6% of Managing Agents' IT estates, an average well below levels seen in wider financial services, many firms are not only investing in major modernisation of core insurance platforms but accelerating cloud adoption. These programmes can strengthen long-term resilience, but they also introduce heightened execution risk, including data validation and integrity challenges cited by some Managing Agents. While firms commonly evidence resilience consideration at project initiation or material change approval, fewer demonstrate how Operational Resilience remains actively engaged throughout the full lifecycle of multi-year transformation.

"A clear theme emerging from this years' self-assessments is increased evidence that Operational Resilience frameworks are well embedded."

This ongoing alignment is critical as scope, delivery plans, dependencies and risk profiles evolve over time.

4. Trends – Areas Showing Increasing Maturity

4.1.3 What's Next

Most Managing Agents have now moved beyond framework establishment. The differentiator for market leaders will be the ability to evidence that Operational Resilience is actively shaping business decisions, investment priorities and risk appetite over time. The test is no longer whether a framework exists, but whether it is demonstrably improving resilience outcomes across the organisation.

4.2 Governance

4.2.1 Context

Effective governance ensures that Operational Resilience is well understood and appropriately prioritised throughout the Managing Agent, enabling decisions to be ratified and clear output shaped for the Board.

In a mature state, oversight and challenge are evident across the three lines of defence, with clear ownership and accountability for IBSs residing with IBS owners within first-line business functions. The Board are regularly trained to ensure they can challenge and sign off the outcomes and position presented in the self-assessment.

As part of regulatory requirements, Board involvement is expected to approve the following:

- The firm's IBSs
- Impact Tolerance statements for each IBS
- Testing output and subsequent remediations and lessons learned
- Forward-looking testing plans
- The Operational Resilience self-assessment on an annual basis and following material trigger events where appropriate

The self-assessment forms a key governance artefact, providing a clear, consolidated point-in-time view of a Managing Agent's Operational Resilience. In a mature framework, it serves as a living document that reflects changes in the operating environment, risk profile and resilience maturity. Through this lens, the document supports Board discussion, oversight and challenge.

4. Trends – Areas Showing Increasing Maturity

4.2.2 Observations

4.2.2.1 Self-Assessment Structure and Content

As part of collating this report, Managing Agent self-assessments were read and reviewed as standalone documents. We noted that overall, the quality of the self-assessments has matured substantially, with templates such as the Operational Resilience Collaboration Group (ORCG) and the Lloyd's 2025 trends report being used as guidance. Formats tended to follow a narrative built on the previous year's position and set out the main elements of an Operational Resilience framework.

However, there were instances where the quality and presentation of the self-assessment made it difficult to clearly understand the firm's current position, resilience maturity or conclusions. This raised questions as to how effectively the firm's Board would have been able to challenge and approve these documents if the content was not as clear, complete and supported as it could have been.

More mature Managing Agents:

- Gave a clear executive summary at the top of the document, outlining the position, and indicating what was new and developed from the last board report.
- Focused on outcomes; directing Board attention to the output of testing and therefore planned activity and investment required for improved resilience
- Included information that was very clear and followed a logical flow - from IBS and ITols, to vulnerability assessment output, testing output, lessons learned and remediation plan.
- Only additional or historic information was stored in the appendix. All key documents needed for full-sign off were available.

Less mature Managing Agents:

- Kept repetitive methodology content which would fit more appropriately in a separate Operational Resilience Framework policy or document.
- Did not make the IBSs and ITols clear at the forefront of the document, making it difficult to measure the testing output against.
- Presented very light or high-level generic testing output making it difficult to ascertain the position of the firm against actual ITols.
- Included key information such as testing output and ITol rationale in an appendix rather than in a prominent position for the board to review and challenge.

4.2.2.2 Independent Oversight, Challenge and Assurance

Operational Resilience independent oversight and challenge remains an area of mixed maturity across the market. Most Managing Agents have established governance structures, with Operational Resilience Working Groups or forums feeding into Operations Committees, Risk Committees and Board-level governance. Roles and responsibilities across the three lines of defence are often defined. However, established governance did not always translate into evidenced independent challenge.

Self-assessments frequently described the design of second-line oversight rather than the substance of the review activity and oversight outcomes. In some firms, there were also indicators of limited specialist capability within the second line to challenge more technical aspects of Operational Resilience, particularly where resilience risks relate to technology, cyber or data.

4. Trends – Areas Showing Increasing Maturity

The clearest maturity distinction was ownership. Less mature firms often continued to rely on Risk or Compliance to drive Operational Resilience activity, even where IBS ownership sits in the first line. While this may have supported regulatory readiness, it was an indicator that Operational Resilience was not sufficiently driven by the business owning the risks and it hindered the evidence of independent second-line challenge. More mature firms showed clear first-line ownership, with the second line providing distinct review, challenge and assurance rather than acting as the engine of framework delivery.

Internal Audit provides an important additional layer of independent assurance. Most firms included Operational Resilience in their audit plans on a cyclical basis, typically every one to three years, and many had completed framework readiness audits ahead of the March 2025 milestone. The next phase of assurance will be important. Positively, follow-up audits tended to be planned or underway for 2026 and 2027, to test whether frameworks are operating effectively in practice, whether governance is driving resilient outcomes, and whether remediation activity is being delivered at pace.

4.2.2.3 Board and Key Stakeholder Training

This was also an area where we observed mixed levels of maturity across the reviewed firms, but with an overall higher degree of training and awareness evidenced at both Board and senior management levels compared to previous years.

More mature firms demonstrated regular and targeted Operational Resilience training programmes for Board members, IBS owners and senior stakeholders, supported by clear and accessible reporting. This enabled Boards to engage meaningfully in discussions, provide effective challenge, and make informed decisions regarding the firm's resilience strategy and outcomes. Regular training programmes for key stakeholders and the wider firm are indicators of an embedded, mature framework.

4.2.3 What's Next

Managing Agents should continue to strengthen governance by sharpening second-line oversight, investing in regular Operational Resilience training for Boards and key stakeholders, and reinforcing clear first-line ownership of IBS outcomes. The IBS owner role should move beyond consultation on framework updates or test scope and become a clear point of accountability for driving resilience outcomes. Where Operational Resilience remains led by Risk or Compliance, firms should consider how accountability can shift closer to the business areas that own the services.

Boards also need clearer, more outcome-focused self-assessments that evidence the firm's current resilience position, the key risks to remaining within impact tolerance, and the remediation or investment priorities requiring oversight. A concise self-assessment should enable meaningful challenge, support better decision-making and demonstrate that governance is translating into improved resilience outcomes.

4. Trends – Areas Showing Increasing Maturity

4.3 Forward-Looking Resilience Assessment

4.3.1 Context

As organisations evolve, so too will the services, resources, dependencies and risks that underpin their IBSs. Under SS1/21, firms are expected to identify vulnerabilities that could threaten their ability to deliver IBSs within impact tolerances, and to use mapping to support both vulnerability assessment and testing activity. Change triggers, horizon scanning and vulnerability assessment are therefore closely linked but serve different purposes;

- **Change triggers** are specific events or developments that may require formal reassessment of IBSs, impact tolerances or supporting resources.
- **Horizon scanning** is the broader forward-looking process used to identify emerging internal and external risks before they crystallise into material change or disruption.
- **Vulnerability assessments** are the structured analysis of where the firm may be exposed, including weaknesses in people, processes, technology, data, facilities or third-party dependencies.

In a mature framework, firms use all three together: horizon scanning identifies emerging risks and potential future triggers; trigger review ensures specific events are identified; and vulnerability assessment translates those insights into targeted testing, remediation and resilience action. This helps embed Operational Resilience into business decision-making, rather than treating it as a retrospective compliance exercise.

Examples of change triggers that may prompt a review include but are not limited to:

- Technology change such as data transformation, migrating to the cloud or new AI adoption
- Merger or an acquisition
- Material incidents affecting IBS delivery
- Regulatory change
- Outsourcing or insourcing a service supporting an IBS
- Any other planned material change that would affect the key resources supporting IBSs (people, processes, facilities, data, technology)

4.3.2 Observations

Framework designs across trigger review, vulnerability assessments and horizon scanning have improved year on year, with more firms setting out clearer processes to identify internal and external developments that may affect Operational Resilience.

However, vulnerability assessments appear to have become relatively static in some firms. While horizon scanning is identifying a broader range of emerging risks, including cyber, technology, data, geopolitical and third-party developments, these insights are not consistently translating into new or refreshed vulnerabilities, targeted scenario testing or remediation activity. This creates a risk that vulnerability assessments become a point-in-time framework artefact, rather than a dynamic assessment of how evolving risks could affect the firm's ability to remain within impact tolerance.

4. Trends – Areas Showing Increasing Maturity

Separately, material changes were often referenced in self-assessment narratives without being clearly identified, assessed or treated as trigger events. Given the level of business change, technology adoption, live incidents and third-party movement seen across the market, it would be unusual for a firm to have no activity during the year requiring formal trigger consideration.

M&A activity is a clear example of an Operational Resilience change trigger. As firms pursue growth across the Lloyd's market, acquisitions and integrations create a heightened period of operational risk across people, technology, data and processes. More mature firms recognised this explicitly, treating M&A as a trigger event, recalibrating IBSs and impact tolerances where needed, refreshing resource mapping, and using scenario testing to assess integration-related vulnerabilities.

4.3.3 What's Next

Managing Agents should strengthen the link between horizon scanning, trigger review and vulnerability assessment so emerging risk insight translates into resilience action. As cyber, third-party, data, geopolitical, climate and technology risks become increasingly interconnected, firms should move beyond monitoring risks in isolation and assess how combined disruption could affect IBS delivery, aggregated exposure and market-wide dependencies. The strongest firms will use these insights to refresh vulnerabilities, update scenarios, prioritise remediation and support Board-level decisions.

Table 01: Example table to express IBSs and ITols in a clear format at the top end of a self-assessment. This includes supporting stats and sub ITols.

IBS	Sub IBS	Impact to Customer ITOL	Impact to Firm ITOL	Supporting Stats	IBS Owners	IBS delgates
Claims	FNOL	XX Days >Quantative measure	XX Days >Quantative measure	X number of claims per week/ per month Peak times		
	Handling					
	Payments					
	Specific COB					
UW	Sub class					
Complaints						

4. Trends – Areas Showing Increasing Maturity

4.4 Impact Tolerances and Sub-Impact Tolerances and Measures

4.4.1 Context

Impact tolerances form a key component of an Operational Resilience framework, providing the benchmark against which a firm's ability to deliver its IBS can be assessed during disruption. They establish the level of disruption that can be tolerated before intolerable harm occurs to both a customer and the firm and therefore provide the reference point for resilience testing. Impact tolerances are supported by a clear rationale that reflects the nature of the service, its customers, supporting stats and the potential consequences of disruption.

4.4.2 Observations

This is an area of positive movement in terms of the market's understanding of the regulatory definitions and identifying and quantifying impact tolerances. In the self-assessments reviewed, firms generally provided a clear rationale that was easy to access, identified vulnerable customers and considered different classes of business. Several examples referred to regulator or market feedback on this area, particularly safety-and-soundness thresholds, and described subsequent recalibration to align better with supervisory expectations or market trends.

We observed more mature Managing Agents beginning to consider sub-ITols where appropriate, enhancing the 'days' measure of an ITol with additional measurements. This could be the number of claimants/ policies or premium indication as an example. However, this newer detail did not often feature in the test output itself.

Less mature firms did not use statistics or volumes in their ITol rationale; this may indicate that these are not therefore carried though to support their testing. For effective testing output, statistics and volumes validate workaround measures, end-to-end processes and provide the best estimate of the reconciliation effort back to BAU.

4.4.3 What's Next

Impact tolerance measures are well understood, and firms should continue to explore ways of augmenting these with relevant statistics, where applicable. With an increased threat landscape and required vulnerability assessments at each cycle, ITols should be subject to rigorous review and analysis, rather than a high level refresh. This good practice lays the foundations for meaningful test design and output in any mature framework.

4. Trends – Areas Showing Increasing Maturity

4.5 Testing with Third Parties

4.5.1 Context

Within an Operational Resilience framework, accountability for remaining within defined impact tolerances sits with the Managing Agent as the regulated entity. As such, the role of third parties is considered in the context of how their services support IBSs and how their performance during a disruption could influence overall resilience outcomes.

Third parties are identified through mapping exercises that identify which external providers support IBS delivery and how critical they are. This typically includes visibility of dependencies, potential vulnerabilities, any single points of failure and an understanding of the level of assurance available.

Resource mapping identifies third parties as named, identifiable components of the end-to-end service, rather than as generic classifications, such as “broker” or “coverholder”. A greater level of specificity supports more meaningful engagement with those entities that are critical to the delivery of IBSs. This enables a clearer view of where reliance is concentrated and where focus may be required.

Consideration is also given to the broader regulatory landscape relating to third-party risk, This includes alignment with PS7/26 Operational incident and third-party reporting, particularly where there is overlap with areas such as third-party risk management and risk registers.

4.5.2 Review Findings

There was a noted increase in third-party engagement across a variety of areas in the Operational Resilience framework, from mapping through to testing. Testing with third parties increased by 30% year on year with circa 60% of the reviewed population having tested third party scenarios in 2025/ 2026. Typically, those Managing Agents regulated under the Digital Operational Resilience Act (DORA) EU scope were found to have adopted a more mature approach to third-party exit planning.

More mature firms have:

- Identified all third parties by entity name and categorised them in terms of how they support IBSs
- Demonstrated a clear engagement strategy with those third-party firms; including communicating the IBSs and ITols and performing vulnerability assessments
- Performed due-diligence and ensured critical third parties have a Business Continuity Plan (BCP) in place
- Validated the third party’s ability to stay within ITols for the IBSs they support by performing joint testing of the dependent service
- Have tested communications in an incident or stressed scenario
- Documented and tested stressed exit plans

4. Trends – Areas Showing Increasing Maturity

We have heard feedback that some Managing Agents continue to find it challenging to secure third-party buy-in for joint testing, particularly for smaller Managing Agents or where providers support multiple market participants. Encouragingly, awareness amongst third parties of the need for resilience testing appears to be increasing, and we have seen strong examples of Managing Agents working with critical providers to test dependent services. There have also been positive examples of Managing Agents sharing test results through the LMA, supporting collective market learning and reducing duplication where appropriate.

Alongside Managing Agent activity, the Lloyd's Market Association (LMA), Lloyd's and London Insurance Market Operations & Strategic Sourcing (LIMOSS) continue to play an important role in raising market-wide maturity in third-party resilience. The LMA's 2026 joint third-party test with DOCOSoft provides a strong example of how collective testing can identify shared vulnerabilities, support remediation and reduce duplication across the market, with further exercises planned for future years. Lloyd's annual Market Wide Scenario Exercises (MWSE) will continue to explore severe but plausible scenarios affecting shared services, working with the market on their design and execution. In parallel, LIMOSS is progressing third-party risk management work to explore a more standardised market approach to supplier due diligence. This could enable suppliers to complete a common set of assurance questions once, with participating firms accessing relevant responses through controlled permissions, rather than issuing separate questionnaires independently.

4.5.3 What's Next

For third parties with high concentration risk across the market, Lloyd's encourages Managing Agents to lean into proactive peer-to-peer testing and share relevant outputs where appropriate to support collective learning. Coordinated testing is most effective when participation is broad and responsibilities are shared; it should not fall to a small number of Managing Agents to repeatedly lead planning and execution while others benefit from the outcomes. Managing Agents should therefore consider how they can contribute proportionately to market-wide exercises, secure internal buy-in from senior stakeholders, increase visibility of the value of joint testing, and remove practical barriers that may limit their ability to participate.

Even where third parties are unable or unwilling to participate directly in joint testing, Managing Agents can still run third-party disruption scenarios to assess their own internal response, workarounds and stressed exit arrangements.

4. Trends – Areas Showing Increasing Maturity

Table 02: Third party and suppliers risk assessment. Informing trackable actions and remediations. RAG is based on the ability to substitute, established workarounds and the potential effect on IBS or ITOL.

Supplier/ System/ Third Party	Status	IBS UW	IBS Claims	IBS Complaint	Notes/actions
Microsoft Azure					RAG indicates workarounds and alternative options and therefore inherent risk to the IBS or ITOL Actions in this column are tracked through and retested once complete
AWS					
PPL					
Whitespace					
Caresmart					
Guidewire					

5. Trends – Areas of Development

5.1 Mature Testing Output

5.1.1 Context

Mature testing output provides clear evidence of how effectively a Managing Agent can remain within defined impact tolerances for its IBSs during severe but plausible scenarios. Over successive testing cycles, a well-developed approach reflects coverage across all IBSs and resource pillars. The testing framework and output forms a central component of a firm's Operational Resilience framework and underpins the narrative presented within the self-assessment.

In a mature framework, test selection is informed by a clear and structured rationale, drawing on known vulnerabilities, critical dependencies and identified workarounds. Testing approaches incorporate varied and mature test types, such as simulations, live exercises and actively testing with third parties. Tests are performed end-to-end including consideration of both business resilience through workaround testing and technical recovery capabilities, timeframes back to BAU and reconciliation processes. Notably, better test outcomes are supported by key statistics e.g number of expected claims, policy and endorsement counts. These allow better validation of workaround effectiveness and give a clear time-measured position on the key question; exactly how long was the firm able to stay within impact tolerance?

5.1.2 Observations

While the observations below highlight significant room for development in the quality of testing outputs, it is important to initially recognise the increased volume and effort being invested in testing activity overall. On average, Managing Agents are now undertaking 6 scenario tests per year, indicating positive momentum in the breadth and frequency of resilience testing. The scenario testing data also shows that coverage of IBSs remained strong and comparable to last year, with 80% of Managing Agents having tested all their IBSs. However, testing across resource pillars was materially less developed with only 36% of Managing Agents having conducted scenario tests that covered all pillars. A key driver for this which makes sense is the reduction of the scenario testing around facilities as the increase in the ease of remote working has led to the facilities pillar being materially less covered within scenario tests this year, followed by reduction in the testing of the people pillar which is more of a concern and which we have covered in a theme below. The testing type split also indicates that desktop and walkthrough exercises remain the dominant form of scenario testing, accounting for 61% of the total tests, compared with simulation tests which represented 39% of tests, which is an increase from previous years. Overall, the data suggests that while Managing Agents are increasing testing activity and achieving broader IBS coverage, there remains further opportunity to deepen testing sophistication, particularly through fuller pillar coverage and a greater proportion of simulation-based and evidence-led testing.

Furthermore, the quality of testing results was found to be a notable area of challenge across the market. The majority of self-assessments reviewed concluded that the Managing Agent was able to remain within

5. Trends – Areas of Development

impact tolerances. However, the statement that a firm "stays within tolerance" is only as strong as the evidence supporting it. Where this conclusion is based primarily on workshops, desktop exercises, assumed recovery timelines or unvalidated third-party dependencies, it should be treated as an informed assessment rather than definitive assurance. Even advanced simulations are inherently assumption-led. Those assumptions are not a weakness in themselves, they are necessary to make testing manageable and repeatable but they should be explicit, challenged and periodically validated.

5.1.2.1 Testing Output
Across the market, we noted a lack of maturity in the testing output itself and a difficulty gaining assurance from the presentation of the testing output in the self-assessments. It was often difficult to ascertain from the data or text presented, how long firms were able to stay within impact tolerances and whether the test incorporated end-to-end processes and recovery time back to BAU. Tests were presented with little detail as to exactly what was tested in terms of resources and IBSs, with a 'pass/ fail' or 'completed' indicator, rather than time metrics, measurements or clear validation of any workarounds used. The regulatory testing template (requested by the PRA FCA in previous years in an excel format), required this information displaying a breakdown of recovery times and metrics. Managing Agents could consider using the same measures in their testing parameters.

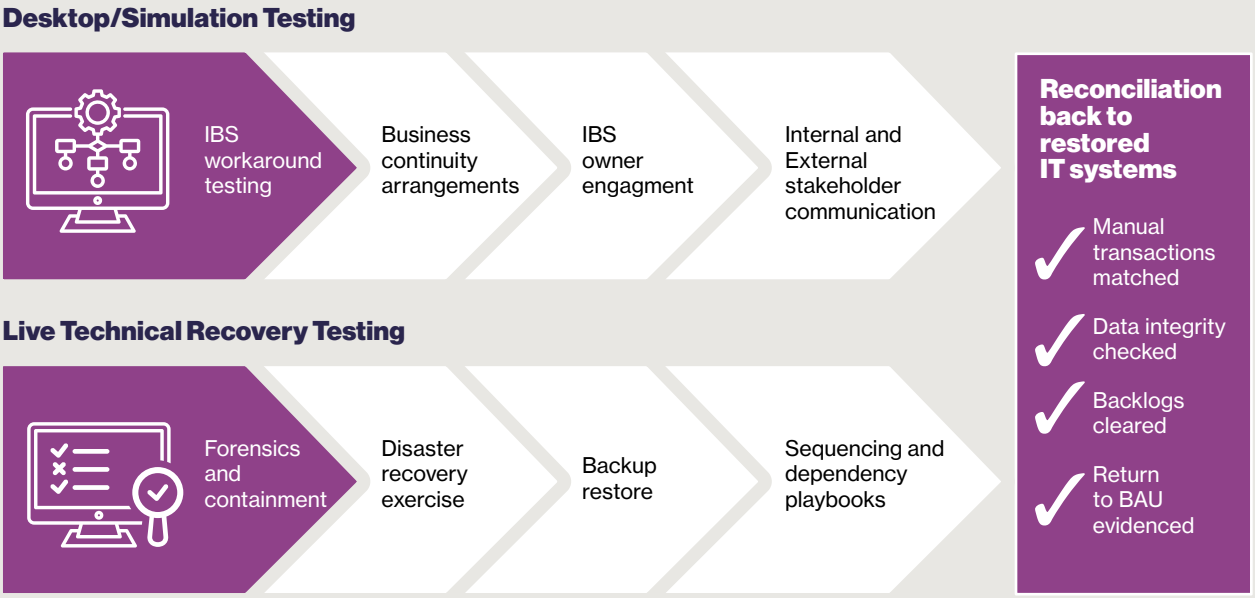
5.1.2.2 Testing Rationale
We saw little movement in this area from last year. In many cases, the self-assessments gave no rationale underpinning the test selection or selected the same tests from previous years. This is possibly linked to where a structured vulnerability assessment performed on the resource mapping was missing, which would then inform the test selection. Testing rationale is a critical part of a testing framework, ensuring known vulnerabilities are tested. A clear methodology as to why tests are selected also helps in resourcing a practical yet robust test plan.

5.1.2.3 Test Resourcing
This is a key area of challenge for firms in the market. Test design and execution is often a skills gap in the Operations or Compliance teams where Operational Resilience typically sits. We saw a notable difference in the quality of test framework and testing output whereby firms had a testing resource. This was both evident in how the testing framework was embedded, and how the tests were designed, executed and written up for the self-assessment.

5.1.2.4 End-to-End Business Process and Recovery Testing
Additionally, we observed a disconnect between desktop or simulation-based testing, which often focused on testing effectiveness of manual workarounds, and live recovery testing of the underlying technology or systems. Both forms of testing are valuable and required to demonstrate end-to-end resilience. However, our review noted that these were not always clearly aligned to demonstrate how business workarounds would operate alongside the actual order, timing and dependencies of technical recovery. Where these tests are undertaken in isolation, it can be difficult to determine whether the firm could maintain the service end-to-end within impact tolerance, particularly where workaround capacity, data reconciliation and return-to-BAU activities depend on the successful recovery of specific technology components.

5. Trends – Areas of Development

Table 03: Aligning Business Continuity and Technical Recovery Testing



5.1.3 What's Next

In this area of continuing maturity, firms can look to develop how they record and present their testing output to enable a Board to understand and challenge.

The template in Appendix A sets out the good practice core information that can be captured to support meaningful testing output and enable effective Board review and challenge.

5. Trends – Areas of Development

5.2 Frontier AI and AI Mapping

5.2.1 Context

Within an Operational Resilience framework, the use of AI (including frontier AI models), is increasingly relevant to how firms deliver IBSs. Following the FCA, Bank of England and Treasury joint statement on frontier AI models and cyber resilience, there is growing emphasis on understanding how AI adoption influences resilience outcomes, particularly where it introduces new dependencies, risks, or failure points.

Third-party and supply chain considerations become increasingly important where AI capabilities may be externally sourced or supported. Through mapping exercises and third-party management, firms have visibility over where AI models are used across their services and how they interact with existing systems and processes. This includes considering how such models may affect the threat landscape, with frontier AI recognised as potentially amplifying certain vulnerabilities (e.g. cyber, data integrity, or decision-making risks).

Governance and oversight also evolve in line with the increasing use of AI. This includes consideration of how Board-level understanding is developed and maintained, ensuring that decision-makers are equipped to engage with the risks and implications associated with frontier AI as part of the wider operational resilience framework.

5.2.2 Observations

In the 2025 self-assessment review and prior, we found there to be little or no mention of internal use of AI, or potential vulnerabilities posed by its use. This year there was a slight increase in frontier AI being recorded, mapped or tested. As an area of rapid development in the market as whole, we did note however, that the mapping or identification of AI in the 2026 self-assessments did not necessarily correlate with more recently published statistics. For example, in the April 2026 LMA Survey on AI Risk Management, the percentage of firms that disclosed their emerging use of AI to support underwriting or claims services was notably higher than evidenced in firm's operational resilience mapping, vulnerabilities or future testing plans. In addition, we noted that firms are not yet evidencing mapping of AI usage by third parties supporting IBSs, which has the potential to further increase the operational resilience risk to the Managing Agent.

More mature firms;

- Have reviewed their IBS mappings to ensure that any AI being used to support the IBSs is recorded appropriately, assessed for vulnerabilities and considered for testing.
- Large scale transformation using AI has been considered as a change trigger and treated as such within their embedded Operational Resilience framework.

5.2.3 What's Next

As an area of rapid market development Lloyd's would expect to see more movement towards Operational Resilience awareness and maturity in this area. With the transition periods of the EU AI Act ending over the next couple of cycles and the Mills review from the FCA published this year, 2026 represents a key period of review in this space.

5. Trends – Areas of Development

5.3 People Resilience

5.3.1 Context

'People' are one of the resource pillars mapped for each IBS, documenting who performs the process tasks. This can be a team, key skills or outsourced teams. In most test scenarios, people are a key element of the scope; whether that be because firms are testing key person dependencies or skills, surge cover, or the people that use and perform work on certain technologies.

5.3.2 Observations

Most Managing Agents tell us that people, expertise and specialist knowledge sit at the heart of their business model and service delivery. While the 'people' pillar was tested in the majority of test plans reviewed, this was often limited to the process steps that people or teams would follow, with less evidence that scenarios explored how people would perform and be supported during prolonged, stressful disruption. There was often an implicit assumption that staff would be able to cope and continue to deliver effectively under crisis conditions, despite emerging industry data suggesting that fatigue, stress and sustained operational pressure can materially affect workforce capacity, decision-making and incident response. There was also limited consideration of how teams would fare where long-term stressors further deplete workforce capacity, or how staff would be supported during a large-scale incident while simultaneously managing workarounds, backlogs, crisis communications and BAU responsibilities. This suggests that the people element of Operational Resilience is still often treated as a process or resourcing consideration, rather than as a dynamic factor that influences how individuals, teams and leaders respond under sustained pressure.

5.3.3 What's Next

Market leaders are moving beyond identifying people dependencies and actively assessing the human impact of prolonged operational disruption. Future testing scenarios should look to consider factors such as stress, fatigue, reduced workforce capacity, competing priorities between crisis response and BAU activities, and the effectiveness of training and support mechanisms for staff. By incorporating people resilience and leadership considerations into scenario design, firms can better understand how workforce wellbeing may influence service delivery during extended incidents and identify opportunities to strengthen preparedness, decision-making, and recovery capabilities.

5. Trends – Areas of Development

5.4 Cyber Resilience and Recovery

5.4.1 Context

Cyber risk continues to be an important consideration within the broader geopolitical and economic environment. Periods of instability can heighten both the likelihood and impact of cyber activity, particularly where firms rely on interconnected technology, data, people and third-party services to deliver critical operations. Threat intelligence also indicates that the nature of cyber risk is evolving, with insider threat increasing, including threat actors seeking to recruit or bribe trusted individuals to facilitate access, and social engineering remaining a primary route to compromise, including helpdesk or IT support impersonation. For the Lloyd's market, a material cyber incident could therefore have significant operational consequences and wider implications for market confidence if critical services are disrupted.

In this context, we asked firms to provide greater detail on their cyber resilience capabilities and cyber recovery arrangements, with particular emphasis on how these are integrated into and support the Operational Resilience framework.

The key distinction is not whether an organisation can prevent every attack, but how effectively it can withstand, respond to, and recover from one. Strong cyber resilience improves an organisation's ability to detect threats, contain impacts, and maintain critical services, but it does not eliminate cyber risk.

5.4.2 Observations

While many Managing Agents demonstrated high levels of cyber maturity, in the current climate, there is no complete protection from all cyber threats. Lloyd's review outcomes showed that even Managing Agents with strong cyber resilience capabilities, such as those achieving high levels of maturity against recognised frameworks such as the National Institute of Standards and Technology (NIST), remain vulnerable to cyber-attacks. In several cases, threat-led penetration testing conducted against formal testing frameworks resulted in all test objectives being achieved, demonstrating that determined attackers can still compromise environments despite mature control frameworks.

More than 87% of Managing Agents reported having implemented immutable backups, either through cloud-native or other backup tooling. However, the evidence of recovery from more disruptive and destructive cyber scenarios was less consistently demonstrated. In particular, fewer firms demonstrated how firms would recover from more complex scenarios where backup environments were compromised, encrypted or otherwise undermined. This means that while backup capability is increasingly established, the evidence base for restoring trusted data and critical systems safely, in the right sequence, in secure recovery environments and within impact tolerance remains more varied in complex disruptions.

5. Trends – Areas of Development

More mature Managing Agents:

- Demonstrated investment in cyber security controls aligned to recognised industry frameworks such as NIST CSF
- Embedded advanced penetration testing such as red-team testing and threat-led penetration testing on an annual basis with circa 80% of Managing Agents having conducted one or more of these tests in the last 12 months.
- Developed a more holistic approach; clear linkages between cyber resilience, disaster recovery capabilities, and the continued delivery of IBSs.
- Considered more advanced recovery capabilities, including recovery playbooks, clear dependency mapping, offline or vaulted backups, minimum viable business recovery arrangements and cleanroom recovery options, to demonstrate how critical services could be restored safely under loss-of-trust conditions.

5.4.3 What's Next

Industry expectation has moved beyond demonstrating that backups exist. Live recovery testing of critical systems supporting IBSs should now be viewed as the baseline expectation, with more mature Managing Agents going further by testing full infrastructure rebuilds under loss-of-trust conditions. This is materially different from traditional disaster recovery, which may validate recovery of specific systems in a controlled environment but does not always prove that the firm can restore trusted technology, data and operating capability following a destructive cyber event. Mature testing should therefore evidence not only that systems can be recovered, but how, in what order, within what timeframe, and with what dependencies to keep IBSs within impact tolerance.

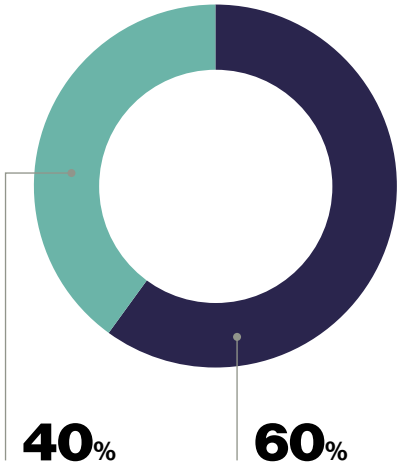
Separately, while paper-based control assurance and documentation reviews continue to have an important role in evidencing the design and governance of cyber controls, the market is increasingly moving towards more dynamic forms of assurance. Lloyd's encourages Managing Agents to complement documentation-based reviews with continuous red team testing activity and threat-led penetration testing, to provide more realistic assurance that controls operate effectively against real-world attack techniques and evolving threat scenarios.

6. Benchmarking Data and Metrics

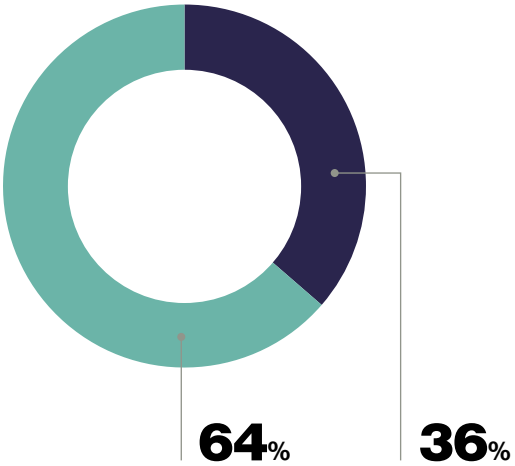
6.1 Scenario Testing Metrics 2026

Average number of tests per managing agent: 6

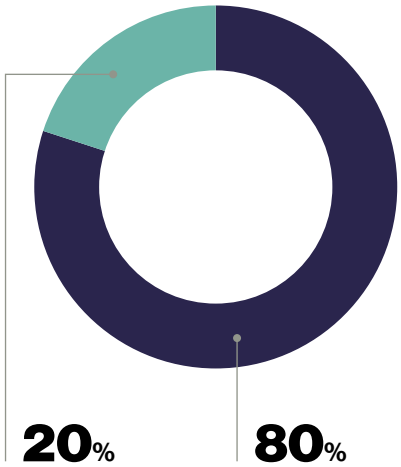
MAs that tested with third-parties



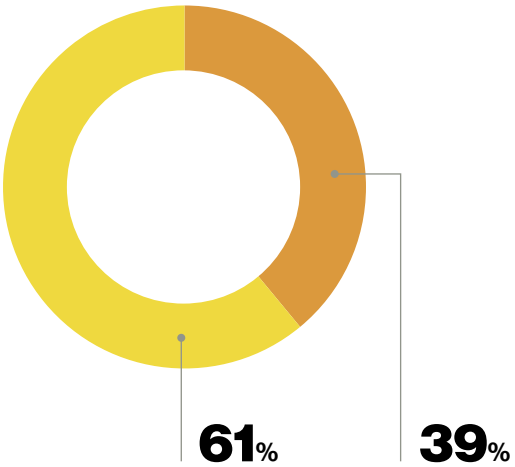
MAs that tested all pillars



MAs that tested all IBS



Split: simulation vs desktop/ walkthrough tests



Yes
No or Unclear
Desktop/Walkthrough tests
Simulation tests

6. Benchmarking Data and Metrics

6.2 IBS and Impact Tolerance Data

The market IBS and ITol benchmarking data has been updated from last year where Lloyd's oversight activity of a Managing Agent's Operational Resilience self-assessment identified a change in its IBS or IToL position.

Individual Managing Agents are not expected to always fit within the market averages but rather present a sound rationale that supports the IBS and ITol selections they have made.

Observations

The material movement in this year's benchmarking is the tightening of Safety and Soundness impact tolerances, particularly at the upper quartile. This indicates that firms are reducing longer-tail prudential tolerance levels, reflecting both market benchmarking and supervisory feedback.

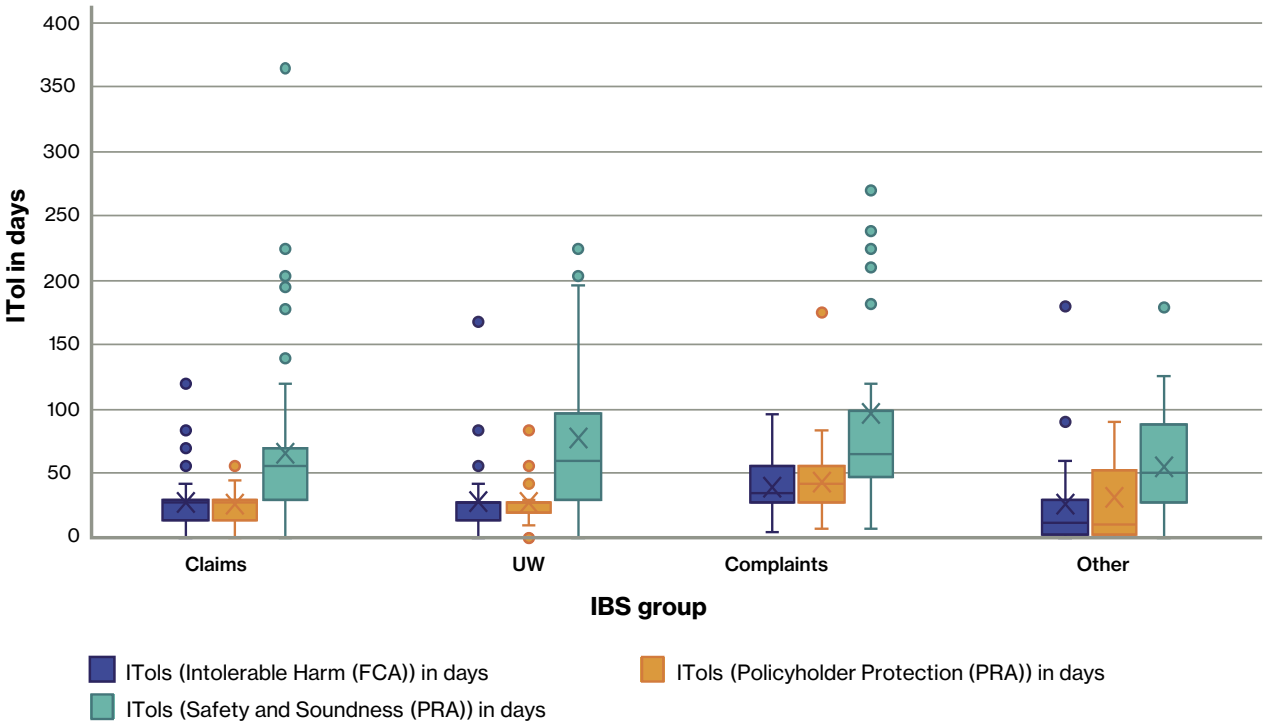
Claims and Underwriting show the clearest evidence of this trend. Claims Safety and Soundness tolerances reduced from 73 to 66 days on average, with the upper quartile reducing from 84 to 70 days. Underwriting also tightened, with average Safety and Soundness tolerances reducing from 81 to 77 days and the upper quartile falling from 114 to 94 days. This suggests firms are moving away from outlier tolerance positions and aligning more closely around defensible prudential resilience outcomes.

Complaints shows a more mixed picture, with Intolerable Harm tolerances lengthening slightly while Safety and Soundness tolerances tightened materially. The most notable movement was at the upper quartile, which reduced from 182 to 97 days. This is a significant reduction in longer-tail prudential tolerance levels and reinforces the broader market trend towards shorter, more supportable Safety and Soundness thresholds.

Overall, the benchmarking gives firms a useful market reference point, but the expectation remains that each Managing Agent should be able to explain and evidence its own IBS and ITol rationale. The strongest positions will be those supported by service-specific data, customer impact analysis, vulnerability assessment and testing evidence, rather than alignment to market averages alone.

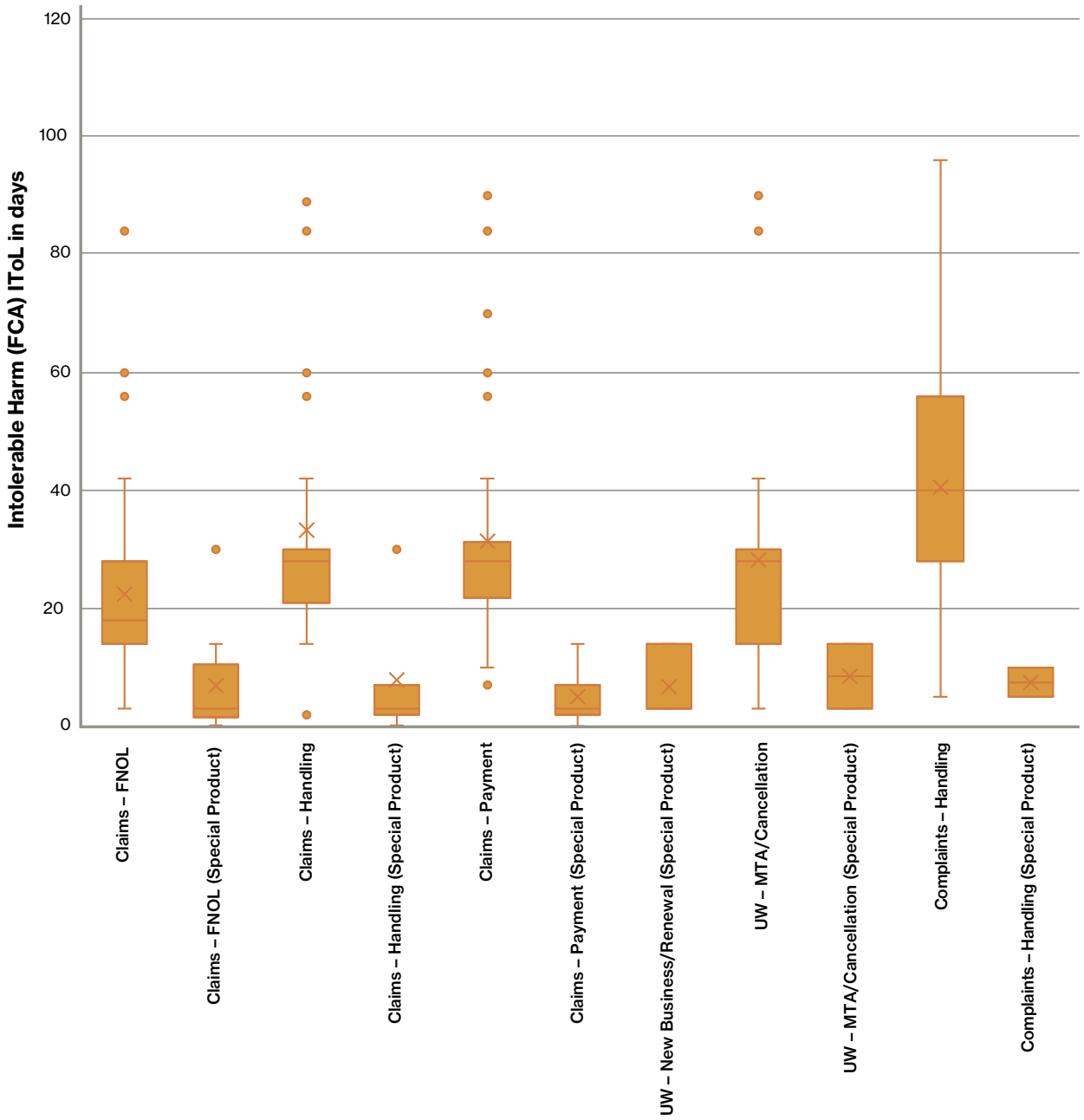
6. Benchmarking Data and Metrics

ITol spread by IBS group



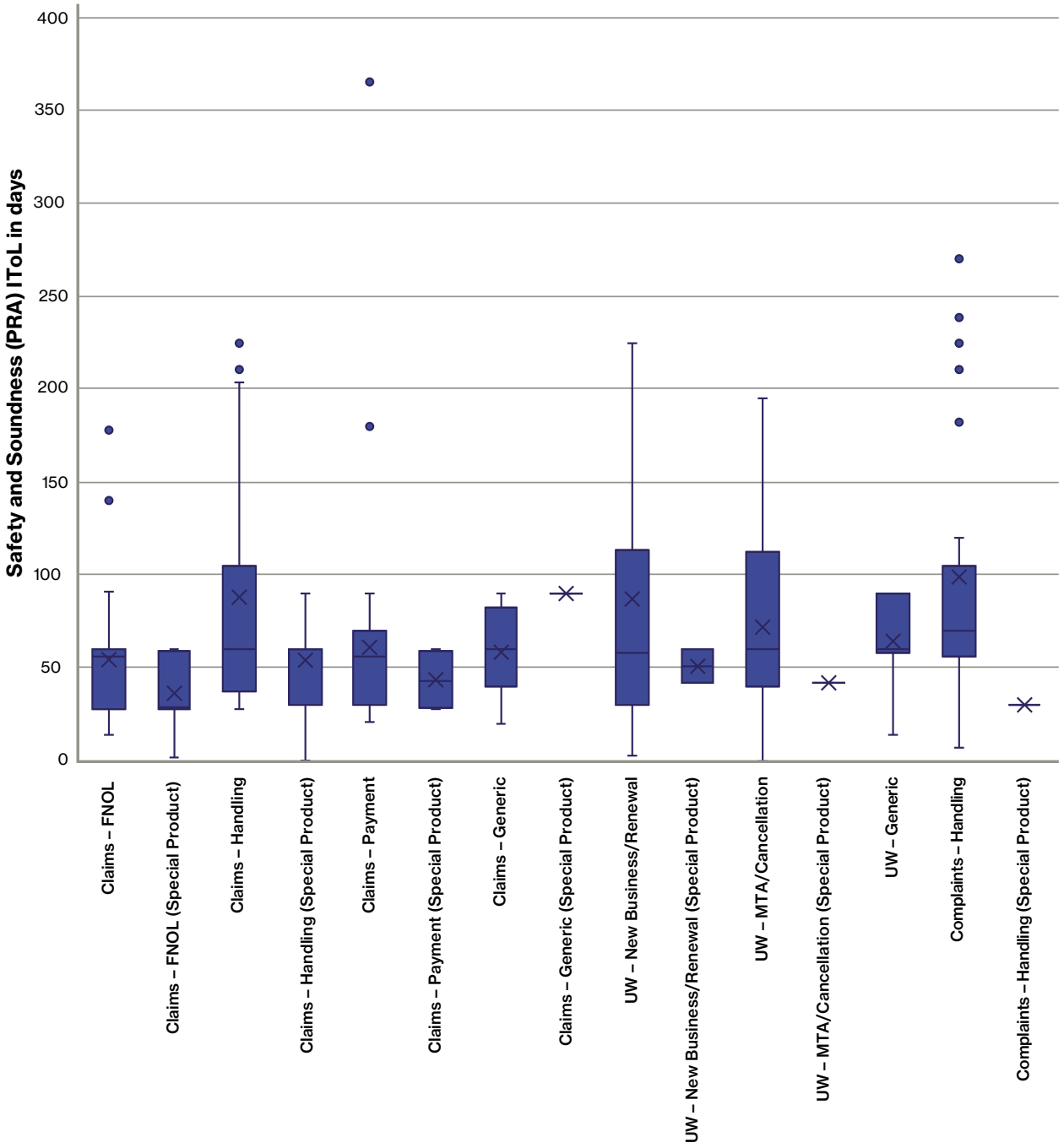
6. Benchmarking Data and Metrics

Intolerable Harm to customer (FCA) IToL spread by IBS type



6. Benchmarking Data and Metrics

Safety and Soundness (PRA) IToL spread by IBS type



7. Appendix A

7.1 Scenario Testing Template

Template Section	Information to capture	
Test scope	Identify the IBSs, resource pillars, and resources (systems, processes, third parties and people/teams) included in scope. Outline how the scenario meets the 'severe but plausible' threshold (such as by having conducted an impact vs likelihood risk assessment)	
Rationale for test selection	Explain why the test was selected, including links to known vulnerabilities, prior incidents, trigger events, horizon scanning outputs, dependency concentration or previous lessons learned.	
Scenario and assumptions	Record the key scenario parameters and assumptions used, including expected volumes, backlog, workaround capacity, third-party response times, data availability, reconciliation effort and any assumed recovery sequence.	
Time-based recovery evidence	Record the time taken, or estimated to be taken, for each recovery step for both business workaround effectiveness and technology recovery.	
	Workaround testing	Describe the workarounds used until trusted technology and data are restored. This can include information such as when workarounds were activated, how long they remained effective, the volumes they could support and any constraints such as staffing, manual processing capacity, data availability or customer communication requirements.
	Technical recovery	Evidence the live technology recovery testing timeline, including the timeline or estimated timeline for incident detection, escalation, forensics, containment, system recovery, data reconciliation and return to BAU order. Timing of system restoration dependencies between systems should typically be based on actual live disaster recovery data.
Outcome against impact tolerance	State whether the firm remained within impact tolerance, supported by evidence rather than a simple pass/fail conclusion. This should be based on the cumulative recovery timeline, including business workaround effectiveness, technology recovery, data reconciliation and return to BAU. The output should also identify the point at which intolerable harm would arise and whether any sub-impact tolerances or supporting measures were tested.	
Lessons learned and remediation	Capture lessons learned, vulnerabilities identified, remediation actions, owners, target dates, governance route and how progress will be tracked to closure.	

Authors

Jess Tasellari

Head of Market Operational Resilience – Lloyd's

jess.tasellari@lloyds.com

Jess leads the oversight of operational and cyber resilience across Managing Agents in the Lloyd's market. Drawing on more than 15 years of experience in banking and insurance, she brings deep expertise in operations, risk management and resilience to drive market-wide resilience outcomes, regulatory engagement and industry collaboration.

Melody Miller

Executive Director- Sea Change London

melodymiller@seachangelondon.com

With 10 years extensive experience across the Lloyd's and London Market, Melody is known for her innovative thinking, stakeholder skills and ability to deliver complex change. She has supported insurers and managing agents through major transformation programmes and is recognised for her expertise in operational resilience, change management, product delivery and stakeholder management.

Sam Nowell

Chief Executive Officer - Sea Change London

samnowell@seachangelondon.com

With a 25-year career in the London market spanning many major transformation programmes, Sam is known for her clarity of thinking, outcome focused leadership and ability to simplify complexity. An AI Ethicist and technologist, Sam's work centres on collaborative transformation across the insurance ecosystem. Sam is a sought after voice on operational resilience and AI Governance.

Glossary

- **AI** - Artificial Intelligence
- **BAU** - Business as Usual
- **BCP** - Business Continuity Plan
- **CMORG** - Cross Market Operational Resilience Group
- **DORA** - Digital Operational Resilience Act
- **DR** - Disaster Recovery
- **EU** - European Union
- **FCA** - Financial Conduct Authority
- **IBS** - Important Business Service
- **IT** - Information Technology
- **ITol** - Impact Tolerance
- **LIMOSS** - London Insurance Market Operations & Strategic Sourcing
- **LMA** - Lloyd's Market Association
- **M&A** - Mergers and Acquisitions
- MWSE - Market Wide Scenario Exercise
- **NIST** - National Institute of Standards and Technology
- **NIST CSF** - National Institute of Standards and Technology Cybersecurity Framework
- **ORCG** - Operational Resilience Collaboration Group
- **PRA** - Prudential Regulation Authority
- **PS7/26** - PRA and FCA Policy Statement 7/26 on operational incident and third-party reporting
- **SS1/21** - PRA Supervisory Statement 1/21 on Operational Resilience: Impact Tolerances for Important Business Services

Useful Links

- The Lloyd's Principle 12 maturity matrix and breach reporting
- ORCG Guidance November 2023 Guidance for Managing agent Operational Resilience - TLP Clear - CMORG.pdf
- LMA Operational Resilience committee documents - including templates, guidance and FAQs
- LMA Survey on AI Risk Management 2026
- PRA Supervision 2026 Priorities
- PRA Supervisory Statement SS1/21 - Impact Tolerances
- FCA Policy Statement PS21/3
- Operational Resilience Trends Report 2025
- FCA, Bank of England and Treasury joint statement on frontier AI models and cyber resilience | FCA
- https://www.fca.org.uk/publications/corporate-documents/mills-review

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.

Instagram Lloyds of London
LinkedIn Lloyds of London
YouTube Lloyd's Insurance