Operational Resilience

Tooling Panorama

2023

The Positive Way

WAVESTONE

Foreword

We are proud to present our third edition of the Operational Resilience Tooling Panorama. This year has marked a big shift for operational resilience with regulation and market forces at the forefront of driving user adoption.

Our analysis of the tooling landscape reviews market trends and outlines challenges that organisations should be aware of when selecting and implementing an operational resilience tool.

Sophy Brady-Halligan
Senior Consultant

Leina Hatch
Consultant

Abdisalan Mahmud
Analyst

2023 Operational Resilience Tooling Panorama

NAVIGATING THE PANORAMA

Tools have been sorted into different operational resilience topic areas. Within each area, tools are further categorised as broad, niche or standard depending on the range of capabilities they offer.

- **Broad** tools have functionalities outside of the topic area
- **Standard** tools only offer functionalities in that topic area
- **Niche** tools focus on specific functionalities within the topic area

The Data

221

Tools across 14 categories, a 15% increase compared to last year

180

Companies included in the radar, a 7% decrease from last year, which could be indicative of mergers and acquisitions

37

New vendors compared to last year

For this edition, we have delved deeper into the tooling landscape to gain a better understanding of the different capabilities offered. To do this, each category has been segmented into 3 different ranges of capabilities covering niche, standard and broad. Our analysis of the current market tooling landscape and experience on the field have enabled us to uncover 4 key trends and challenges.


01
The Trends

Top 4 Trends

01 Tools have evolved to cover a broad range of resilience capabilities

Market leaders in operational resilience tooling are increasing the scope and value of their offerings through M&A activity, leading to an increase in tools that act as a 'one-stop-shop' for operational resilience

Are you looking for a broad tool?

Focus on our risk management, resilience planning and crisis monitoring & response categories

02 TPRM tools are maturing beyond end-to-end lifecycle management

As regulators increase focus on third party dependencies, there has been an increase in the number of tools offering third party resilience and third-party risk management capabilities

Are you looking for a third-party tool?

See third party resilience or the broad and standard sections of risk management

03 Regulatory demands are driving the need to visualise resilience gaps

Vendors are increasingly offering IBS dependency visualisaton tools, with some also offering connected incident management or testing functions to aid resilience testing of dependencies

Are you looking for an IBS mapping tool?

Look through our important business service mapping section or the broad section of resilience planning

04 The need to self-certify compliance is leading to new MI & reporting features

A small portion of vendors have begun to offer new MI & reporting activities to support self-assessments, but exisiting MI capabilities are limited and require improvement

Are you looking for an OpRes MI tool?

Find our resilience planning and risk management categories

01 Tools have evolved to cover a broad range of resilience capabilities

Overall, around 1/3 of market tools cover broad capabilities. Last year there was a rapid consolidation of the market through M&A activity, and in 2023 this trend continued but only for specific categories such as risk management and resilience planning.

Our broad range refers to tools covering more than one resilience capability such as business continuity, incident response, risk management, disaster recovery, crisis management or business process management. It can be worth considering a broad tool for organisations looking to bring everything that is under operational resilience into one platform.

Big players in the market are continuing to expand their offerings to further increase their appeal. Two key examples of this in 2023 include a leading tool provider within Integrated Risk Management (IRM) solutions and another leader within crisis management and critical business communications. Both organisations have each acquired smaller firms that specialise in top-tier business continuity, operational resilience, and risk management capabilities to integrate into their existing platform offering.

This is interesting for organisations who plan to embed BAU operational resilience into existing risk functions as tools within this sphere seem to be designed to help facilitate this transition.

For organisations looking to find one tool to manage their operational resilience, we recommend looking at tools under our risk management, resilience planning and crisis monitoring & response categories. We see this trend remaining as the tooling landscape continues to consolidate itself.

02 Third-party risk management tools are maturing to go beyond end-to-end lifecycle management

32 tools cover third party risk management with over half of them entering our radar this year.

Around 76% of tools in our risk management category cover third-party risk management showing a strong shift to meet regulatory demands.

Regulators are drawing greater attention towards third party risk and its connection to third party resilience. Financial services firms are required to document all third-party dependencies for IBSs, perform risk assessments, and conduct due diligence to inform on concentration risk exposure. UK regulators are also requiring firms to include critical fourth parties in risk assessments.

Most tools in our broad range category cover end-to-end third-party lifecycle management. Some tools within this category cover fourth parties and concentration risk. For fourth parties, tooling capabilities include storage of fourth-party information into a central repository, functionality to conduct due diligence assessments and visual mapping of fourth party dependencies. Compliance monitoring and audit management are also included in broad tools where a focus is on risk remediation progress to demonstrate resiliency which will increasingly become a decisive factor for contract negotiations and renewals.

Our standard range includes tools that cover the end-to-end third-party lifecycle management process with risk assessments, vendor due diligence workflows, reporting and analytics. Tools in this range are offering access to data intelligence networks to supplement ongoing monitoring, risk evaluation and assessments. Data intelligence networks enable organisations to obtain a 360-risk view on each vendor through dynamic dashboard reporting.

Other technologies such as automation, data analytics and AI are also commonly found in standard tools. Automation appears to be mostly being applied at the screening and onboarding process. Data analytics seem to be used for vendor selection, risk assessments, performance monitoring and compliance monitoring. AI can be used for intelligent vendor onboarding, due diligence, contract analysis, risk scoring, compliance, and continuous monitoring. A use case could be configuring resilience response workflows using a “if this happens, then do that” programming for when risks arise.

Niche tools for this category covered certain aspects of the lifecycle process including vendor performance management, supply chain risk management, mitigation measures like escrow but also an increased focus on cyber security risk management.

As regulation increases its focus on third-party cloud computing providers, we expect to see some TPRM tools offering features to integrate cloud estate in the near future. Organisations should begin to shift from a compliance-driven mindset to a risk-driven mindset by anticipating this need early.

03 Regulatory demands are driving the need to visualise resilience gaps through IBS or critical functions mapping

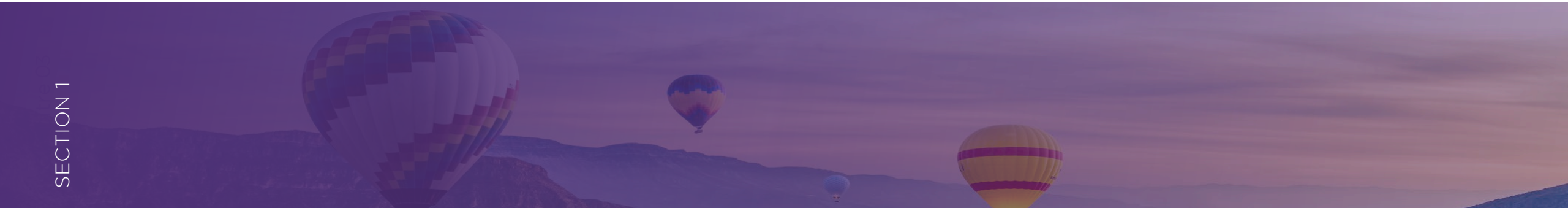
IBS mapping is a new category addition to our radar with a total of 6 tools covering niche, standard and broad business process mapping capabilities.

Our broad range covers tools that offer scenario testing simulations in addition to standard business process mapping functionalities. The most popular tools on the market are leading enterprise architecture management suite tools that cover multiple capabilities such as governance, risk and compliance (GRC), business process analysis, business capability management, cyber security, and risk management. These tools include collaboration and communication functionalities with customisable workflows and feedback loops. Another capability that falls under this range is reporting and analytics.

Broad tools appear to offer a customisable view to focus on operational resilience matters and seem to embed with other resilience capabilities like business continuity and operational risk management.

Our standard range covers process modelling, process analysis, process optimization workflows and integration capabilities with other systems to provide a holistic view of an organisations operational resilience posture. A tool in this category must offer the possibility to map process and technology dependencies and offer drill down functionality for detailed mapping.

Niche tools in our radar cover specific functionalities like compliance mapping, performance monitoring, supply chain analysis as well as application or technology mapping. A niche tool is worth considering for companies looking to embed a specific functionality into their existing tooling landscape.



04 The need to self-certify compliance is leading to new MI & reporting features

- **Our broad range** includes, in addition to those covered in our standard range, functionalities such as KRI libraries for risk management as well as a focus on corrective actions and measures to implement for mitigation and remediation efforts

- **Our standard range** showcases risk assessments and real time monitoring for risk management tools whilst tools for resilience planning offer self-assessment reporting

- **Our niche range** of tools cover compliance mapping functionalities and compliance checklists against leading industry standards for cybersecurity (i.e., ISO 27001, NIST…) and operational resilience

We see this trend continuing to evolve and converge with operational risk with new reporting types being gradually introduced, notably around testing

18%

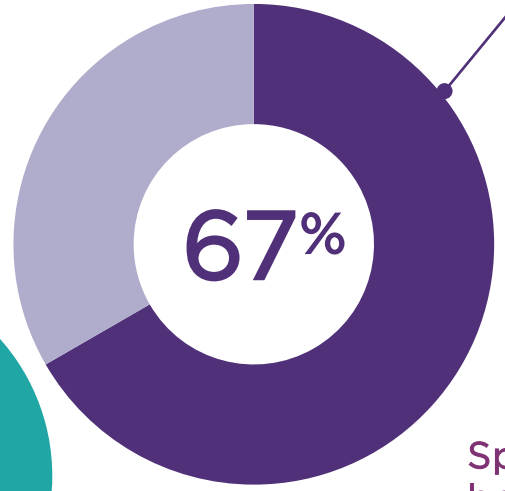
of tools in our radar under our resilience planning and risk management categories cover self-certification functionalities. This shows that there is still room for progress between now and 2025 as financial services firms in the UK approach the FCA's operational resilience compliance deadline and firms in Europe prepare for DORA.


02
The Challenges

Top 4 Challenges

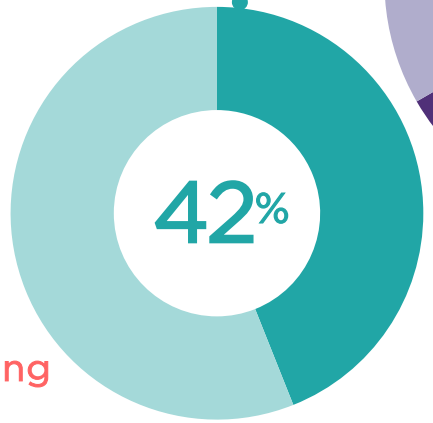
Struggle to implement consistent MI & reporting capabilities

Most firms continue to use KPIs to report on resilience, with very few effectively implementing KRIs. Those who do have KRIs find it difficult to demonstrate how they move to quantify benefits and impacts on remediation actions.



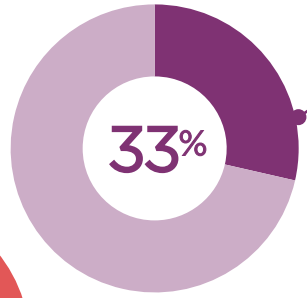
Lack a standardised approach to mapping IBS within existing tools

Organisations struggle to agree on a consistent or standardised approach to mapping IBS within tools.



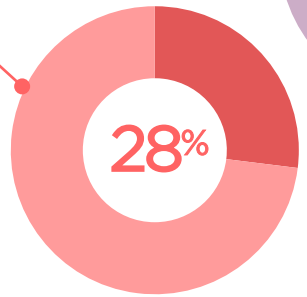
Spend 1-2 years deciding between developing an in-house vs. adopting a market tool

Some firms who have developed in-house tools find that solutions are being used as document repositories. Adopters of external tools are either augmenting their existing tooling landscape with niche tools, or are pushing broad tools beyond their intended uses.



Challenging to consolidate their existing tooling landscape

Organisations that want to build a global overview of their resilience levels struggle to connect and integrate their existing tools within IS landscape.



01 Organisations can spend 1-2 years deciding between developing an in-house tool vs. adopting a market tool

Organisations face two options when looking to adopt an operational resilience tool:

1. Develop a tool internally
2. Customise an external tool

To make this choice, organisations must develop a view of their operational resilience tooling needs, existing tooling capabilities and then identify necessary functionalities to bridge the gap between the current and desired tooling state.

What we have seen work is helping clients assess their tooling requirements to identify if a compromise is possible between desired functionalities and what a market tool offers. Another approach that has worked well is adopting an external tool to cover a niche capability (e.g., business process mapping) and integrating it into a client's IS landscape.

A common mistake we see clients make when implementing a market tool is to stretch it to perform beyond its intended functionalities. This approach often results in over expenditure of resources in the long term and is prone to occur more to clients working in agile delivery. Clients who have developed internal tools often find that users treat the tool as a document repository, and do not make the most of developed functionality.

> **It is important to note that each client tooling landscape is both complex and unique. Hence, a deep analysis is required to explore the different options available with the support of enterprise architects to ultimately avoid technical debt from 'rushing to adopt a tool'.**

02 Organisations that want to build a global overview of their resilience levels are struggling to consolidate their existing tooling landscape

A practical hurdle encountered by some organisations is the ability to integrate and connect existing tools within an IS landscape to help build a consolidated view of overall resilience levels.

It is common to see multiple internal tools deployed within client tooling landscapes each covering different resilience scopes.

This issue is crucial for organisations wishing to automate reporting of their resilience levels using key maturity indicators (KRIs and KPIs) to top management. Attempting to build an internal tool with API capabilities that can provide true integration, and which has the dynamism to provide useful MI or KPIs, would be difficult for most organisations.

As a result, most companies are turning to the market to purchase tools which promise dynamic MI features. However, there are few tools with fit-for-purpose MI capabilities currently on the market.

For those organisations that do opt to develop tools internally, clients should carefully consider what they wish to achieve with tooling for operational resilience and consider viable strategic options around data modelling and data management. Our experience has revealed this as a fundamental requirement to ensure efficient utilisation of existing resources and avoid technical debt. Other key considerations for this challenge include digital and data barriers with re-architecting or re-purposing of data but also options on how to store operational resilience data (via data warehouse or a data lake).

03 Addressing consistent MI and reporting capabilities continues to remain a complex issue for organisations

Around 45% of tools in our tooling radar claim to offer MI and reporting capabilities.

However, clients with tools already in place are noticing that MI is not always included in tooling packages and when it is, the capabilities offered are minimal with numerous barriers remaining. Another challenge in this sphere remains the ability to effectively implement KRIs with most firms relying on KPIs to report their resilience efforts.

To drive important decision making, firms will define key risk indicators (KRIs) to build a global view of resilience levels throughout the operational resilience lifecycle for top management reporting. In general, these indicators are fuelled by numerous data feeds covering all the resilience capabilities within a firm.

Organisations have yet to master the ability to accurately calculate KRIs and demonstrate how they move by quantifying benefits and impacts on remediation actions as without this, top management will remain unable to prioritise the remediation of resilience gaps.

This category has a lot of maturing and improvement to make over the next year.

04 Organisations are struggling to agree a consistent or standardised approach to mapping IBSs within tools

To ensure compliance before regulatory deadlines, many organisations chose to identify and map business services at the divisional level, rather than at a Group level.

While Group Operational Resilience programmes often set standards and expectations for identifying and mapping business services, organisations still encountered differences in divisional approaches.

In our experience with clients, we have noticed that divisions have mapped IBS dependencies to different levels of granularity and have sometimes used inconsistent frameworks and taxonomies. This issue can become a significant setback for organisations looking to implement a common tool to consolidate IBS mapping Groupwide.

For instance, mapping processes at multiple levels of granularity can be hard to accommodate in a tool that has a singular 'process' parameter. Without a consistent approach agreed prior to acquiring a tool, organisations at Group level will experience setbacks and delays during implementation leading to missed opportunities and poor return on investment.

A secondary barrier to consider is change management. Certain divisions or business units may be reluctant to adhere to Group practices and instead choose to follow their own established approaches, or even refuse to rollout tools to their division. Once clients have learnt how to overcome this challenge, adopting a tool to cover IBS mapping and other resilience capabilities will become a more seamless and straightforward journey through groupwide alignment.


03
Future Outlook

Future Outlook

Our analysis and experience within the tooling field suggests 3 key projections on tooling for the future

1. **MI Functionality**
   Niche tools with purposefully designed MI functionality will begin to emerge on the market.

2. **Broad Tools and Resilience Testing**
   Broad tools will increasingly offer resilience testing modules that may not be fit-for-purpose.

3. **Risk and Third-Party Risk Management**
   Risk management tools will begin to improve third party risk management functionality and fourth party management for reducing the likelihood of systemic risks.

3 future projections

1 Niche tools with purposefully designed MI functionality will begin to emerge in the market

As organisations transition from Operational Resilience programmes into BAU, the need to have continuous and automated monitoring of the resilience of their organisation will increase. We suspect that this, along with MI and KRI reporting, will continue to become a key concern for organisations over the next year or two. In response to market need, we anticipate the emergence of new tools that provide a complete and accurate view of resilience gaps; which quantify the potential financial, reputational, regulatory and customer impacts associated with those gaps; and offer a functionality which supports escalation and reporting of those risks to management.

2 Broad tools will increasingly offer resilience testing modules that may not be fit-for-purpose

Following the release of the recent FCA discussion paper "DP3/22 Operational resilience: Critical third parties to the UK financial sector", which outlines a measure to introduce tools for testing the resilience of material services that CTPs provide to firms and FMIs, we expect to see a rise in the number of broad tools offering testing modules. Some tool providers are already taking this approach, and in our experience, these testing functions are modelled after traditional incident management and escalation tools with a 'simulation' option included, which promise to facilitate resilience tests. Broad tools, however, may not be fit-for-purpose, and we believe that niche testing tools, purposefully designed for resilience, will be better suited to address needs in the longer term.

3 Risk management tools will begin to improve third party risk management functionality and fourth party management for reducing the likelihood of systemic risks

If the FCA brings into force the minimum resilience standards for designated CTPs, as outlined in the recent DP3/22 discussion paper, then risk management vendors may tailor their offerings to reflect the new regulation. For instance, if the FCA increases powers of Financial Service firms to request evidence of critical third-party business continuity capabilities, then risk management vendors may update the TPRM modules accordingly. Alternatively, if the FCA implements the 'framework for the supervisory authorities to identify potential CTPs', vendors may identify an opportunity to begin tackling systemic risk by increasing functionality to manage fourth parties or identify cloud concentration risks, which is a trend that is already beginning to evolve.

Final Thoughts

HOW CAN WAVESTONE SUPPORT?

Tooling is integral to maintaining and streamlining business-as-usual Operational Resilience activities. However, incorrect selection or use of operational resilience tools can introduce unnecessary complexity, errors and sunken costs.

At Wavestone, we have helped our clients to understand specific tooling requirements, conducted bespoke reviews of the tooling market against requirements, and developed implementation and roll-out roadmaps to support the transition to business-as-usual.

If you would like help navigating our tooling panorama, are interested in better understanding the tooling landscape, or would like to understand more about the potential benefits and pitfalls of implementing resilience tooling, please get in touch!

Business , Technology and Sustainability

15 offices
9 countries

4,000+
Employees

Contact our experts

Sophy Brady-Halligan
Senior Consultant
Sophy.Brady-Halligan@wavestone.com

Leina Hatch
Consultant
Leina.Hatch@wavestone.com

Abdisalan Mahmud
Analyst
Abdisalan.Mahmud@wavestone.com