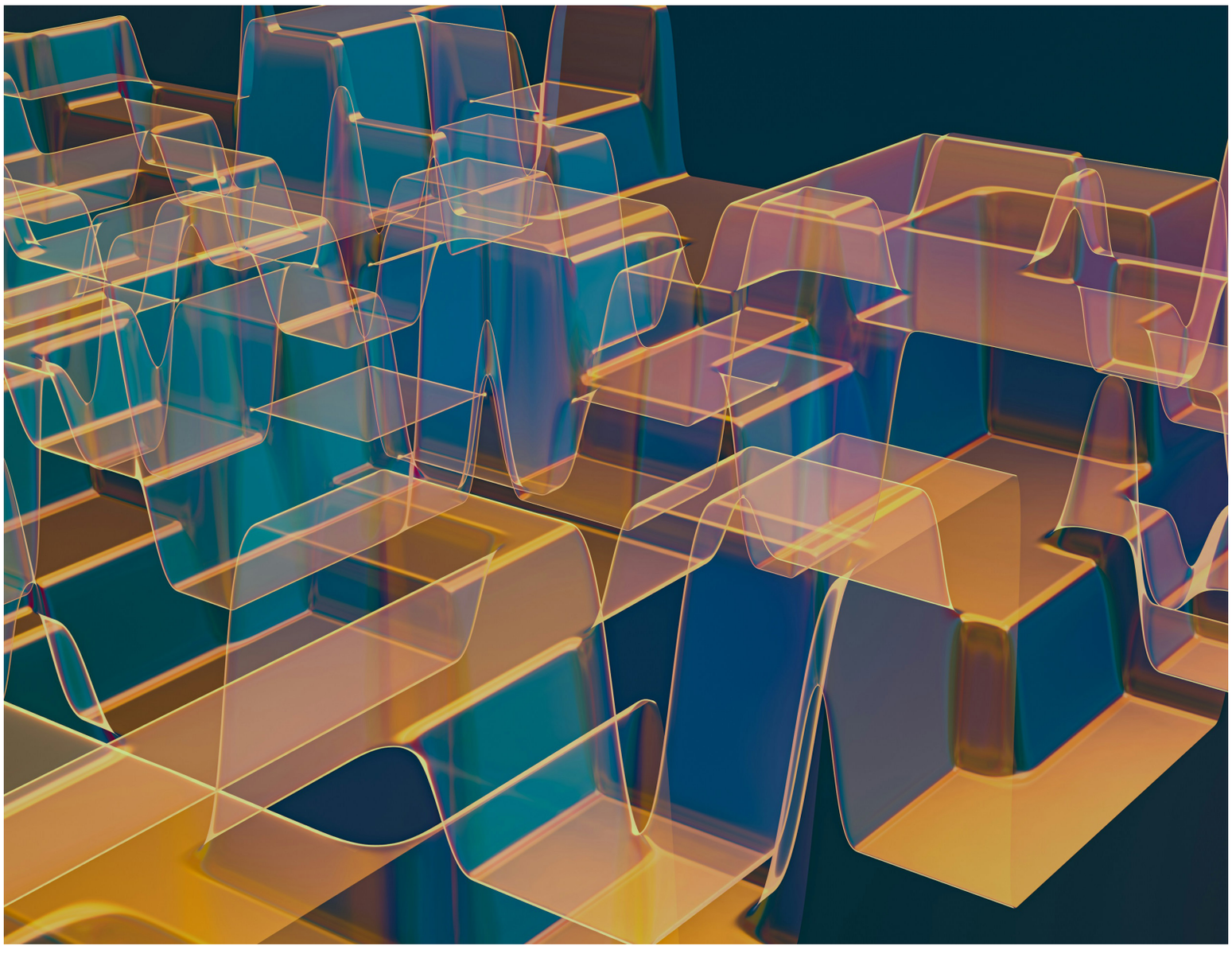
Risk

REPRINTED FROM

Risk.net

Risk.net August 2025



Regional banks favour scenario analysis over op risk modelling

Regional banks favour scenario analysis over op risk modelling

Domestic and smaller regional players favour scenarios to gauge tail exposure; G-Sibs stick to modelling, for now. By *Jin Ye*

Regional banks show near-universal adoption of scenario analysis to gauge their exposure to operational risks, with an average deployment rate of 92% across their top five op concerns, including cyber risk.

They also boast the highest library refresh rates – more than their larger super-regional peers or global systemically important banks (G-Sibs), across the same risks – with precisely three-quarters changing their scenarios across all risks within the past 12 months.

The findings come from the 2025 Operational Risk Survey from Risk Benchmarking, which canvassed 39 banks across five major operational risk categories. Participants comprised 11 regional banks, 11 G-Sibs, 12 super-regionals, and five international financial institutions (IFIs) (See figure 1).

Across all banks, scenario analysis is most entrenched in information security, where 94% of firms use it. IT disruption follows at 89% and resilience risk at 87%. Third-party risk shows moderate uptake, while change management ranks last.

More than half of banks rely on scenario analysis as their primary tool for gauging tail exposure across all five operational risk categories, with resilience risk the clear leader at 85%.

Refresh cycles are fastest for cyber risks: 88% of lenders updated IT-disruption scenarios, and 81% refreshed information security in the past 12 months. Over three-quarters of banks cite periodic review as the trigger.

Confidence, as expressed on a 1–5 Likert scale, is highest in information security, where 80% are very or somewhat confident, a ranking of 5/5 or 4/5 respectively; and resilience, where 78% say the same.

Among cohorts, regional lenders remain the clear leaders in both adoption and library upkeep, averaging 92% usage and 75% refresh across five key operational risks. For information security, 90% reported library refreshes.

G-Sibs follow closely on average adoption and refresh rates, although usage varies more sharply by risk type. They lead on the proportion using scenario analysis as the primary method in determining tail risk – 82% on average, slightly ahead of regional lenders.

Super-regionals lag meaningfully on all three measures. Their average adoption rate is 66%; refresh rates trail at 67%; tail-risk reliance is even lower, at 50%.

IFIs show results broadly similar to super-regionals, although their small sample size makes direct comparison less precise.

Benchmarking brief: Scenario analysis has long been a core component of banks using the advanced measurement approach for op risk capital modelling – although regulatory tolerance for its use to underpin calculations varied sharply between the US and the rest of the world, under the outgoing risk capital regime.

That suggests its use by regional banks, less likely to have built a capital model or follow a stricter loss distribution approach (LDA), serves other purposes. A separate, multiple-selection question on modelling approaches – 'What method do you use?' – sheds light on how scenario analysis sits alongside modelling for our survey contingent.

Across the sample as a whole, the scenario analysis method dominates, outpacing LDA or regression modelling techniques for most risks and cohorts. But regional banks lead by a wide margin, with over 70% selecting scenario analysis for all risks. G-Sibs rank second, showing strong usage over 60% in cyber and third-party risks, but falling sharply for change management. Super-regionals rarely exceed 33% in any category.

This tiered ranking – regionals first, G-Sibs second, super-regionals last – holds consistently across risk types. Stricter modelling use skews toward G-Sibs, particularly in IT disruption, where they outscore regionals 45% to 18%. Regionals use modelling selectively; super-regionals report low uptake across the board.

When comparing the two, data reveals strategic distinctions: while regional banks remain overwhelmingly scenario-driven, G-Sibs balance scenario analysis with modelling in targeted areas, and super-regionals trail both on usage of either method.

Survey responses on confidence levels reveal further nuance.

Among G-Sibs, super-regionals and IFIs, scenario analysis earned a higher percentage of positive confidence scores than modelling across all risk types.

One super-regional risk executive noted: "We moved to structured scenarios this year using the MSTAR Model provided by the vendor Elseware. This has improved our confidence in the models, and, as the data inputs mature, the confidence rating will improve."

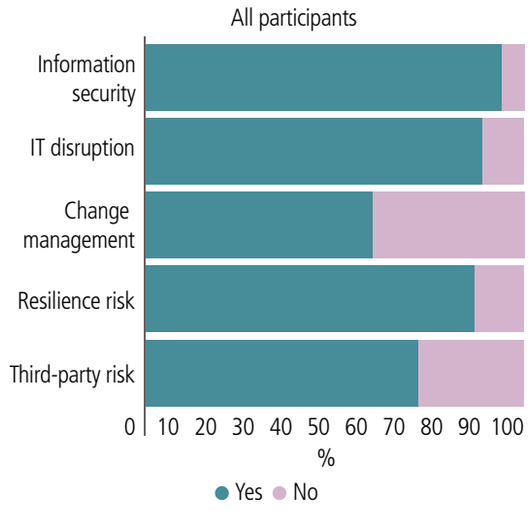
For regional banks, however, risk executives appear less confident in their deployment of scenario analysis in their most adopted areas – for example, cyber risk, where, despite broad use, strategic integration remains limited.

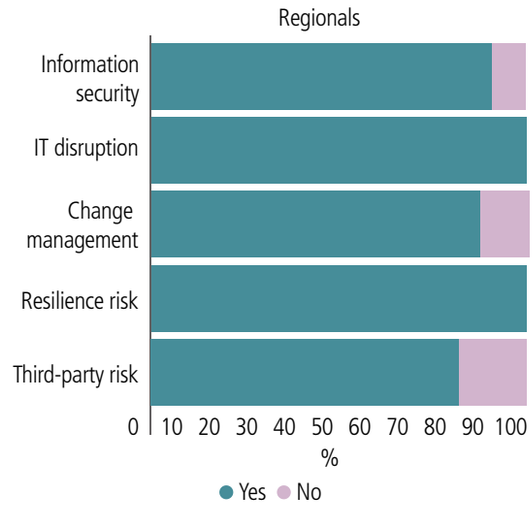
More than two-thirds of banks run group-level scenarios for information security (78%), resilience (77%) and IT disruption (71%). However, a smaller share uses these exercises to set risk appetite – just 61%, 62% and 67% respectively.

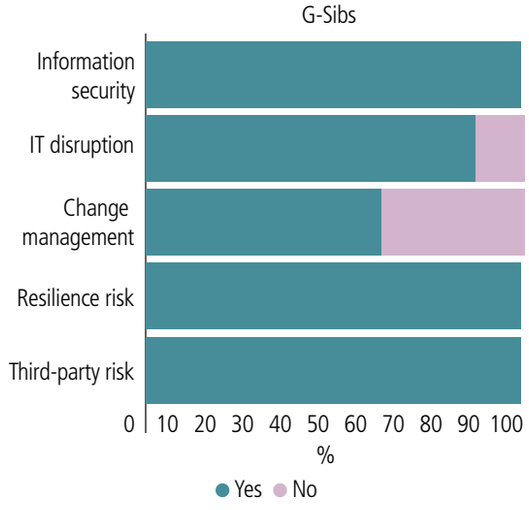
Business lines are the most consistent participants in scenario exercises (78–93% across risks), followed by operational risk heads. Chief risk officer involvement is stronger in resilience (62%), but falls below 30% for cyber scenarios.

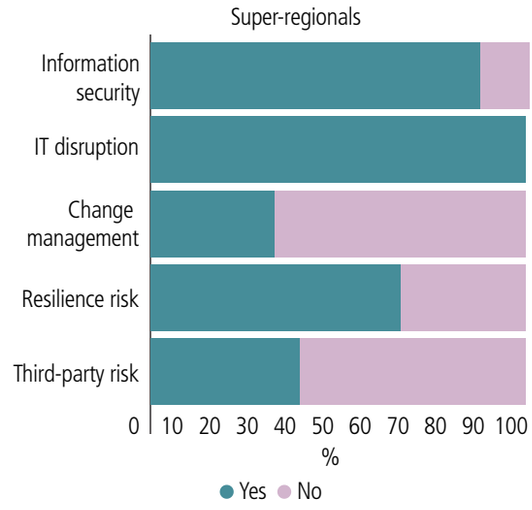
"There is definitely room for improvement regarding senior management involvement in such scenario reviews," said one respondent. ■

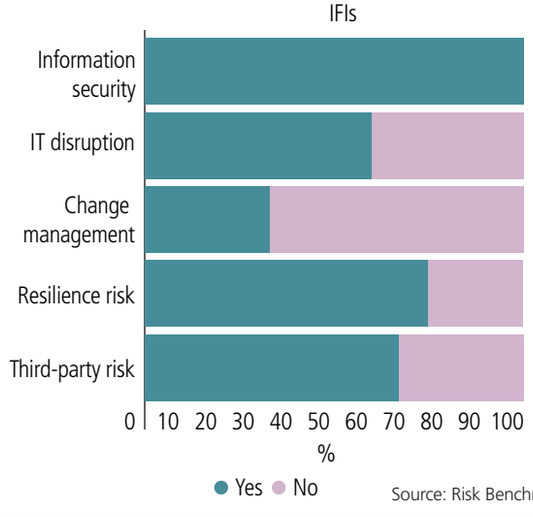
1 Do you use scenario analysis to support measurement of exposure to this risk type?











Source: Risk Benchmarking

This is the third edition of *Risk.net*'s Op Risk Benchmarking service focused on operational risk management practices at banks – the first to combine findings from G-Sibs, super-regionals, domestic banks and IFIs.

Our team engaged in detailed follow-up surveys with 39 respondents about how they manage the top five risks selected by their peer group in our annual Top 10 Op Risks poll, from staffing to technology, modelling to reporting. The Op Risk Benchmarking service is built on the findings of those surveys. Responses were gathered during the second quarter of 2025.

Get involved: This article is one of a series of highlights articles exclusive to Risk Management premium subscribers. Only Op Risk Benchmarking participants get to see the full dataset. If you're interested in joining the next round or hearing more about other Risk Benchmarking services, or have any feedback, please email: benchmarking@risk.net

Editing by Tom Osborn