

# THE KNOW LEDGE

## ▶ SCENARIO ANALYSIS

In this issue, we look at the complex ideas behind scenario analysis. Pundits claim it signals a new way forward for risk managers, building on traditional risk analysis methods. But how many organisations are actually using it?

### **THE SURVEY** *p2*

Risk managers tell us how they use scenario tests and whether they plan to do more

### **THE INTERVIEW** *p10*

Former OECD strategist Angela Wilkinson explains the theory in plain English

► THE SURVEY

# And now for something completely different

Unlike conventional risk analysis techniques, scenario planning challenges risk managers to develop flexible frameworks and look beyond the usual evidence base. But is it catching on?

Armageddon – the day you never thought would arrive. It is likely to evoke feelings of fear in all of us. The stress hormone cortisol rises rapidly, your heart beats faster, vision becomes blurry, hands sweat, mouth goes dry. Panic sets in. You thought this would never happen to you.

Now, imagine experiencing the same scenario, only this time after a dress rehearsal. You know the part you have to play, everyone knows theirs too and you are confident you can ad lib if necessary. In other words, you are a risk manager and you have implemented scenario planning as a key tool in your risk management toolkit.

A conventional risk analysis might involve scenarios, but this means the models have a baseline projection with variations from the norm. There is quantifiable uncertainty and from that, risk managers will be able to perform standard, conventional risk analysis, usually with three types of scenario – that is, high, medium and low risk.

“Imagine experiencing the same scenario, only this time after a dress rehearsal. You know the part you have to play, everyone knows theirs too and you are confident you can ad lib.”

Scenario planning ignores this rule of thumb and instead challenges risk managers to develop a set of flexible frameworks, adaptable to changing baselines and alternative outcomes at each turn. In this issue of *The Knowledge*, experts argue that this is the way forward for risk managers, as it allows planning to be incorporated flexibly. Scenario planning is about looking beyond the usual evidence base that’s used for the risk analysis and asking the ‘what if?’ questions instead.

Email [william.sanders@nqsm.com](mailto:william.sanders@nqsm.com)

Our latest survey of risk managers shows that in the main, more than half (57%) use scenarios to test both emerging and existing risks as a combined product, while 33% test only existing risks.

In a world where it seems like a new risk emerges hourly, it is interesting to note that only 9.5% use scenarios to test new, emerging risks as a standalone risk.

When asked how many scenario tests are conducted each year, respondents gave answers ranging from a few to hundreds or thousands. Size of firm and appetite risk could be responsible for these differences, though it is not clear from the results.

When it comes to planning ahead, more than half (55%) expect an increase in scenario analysis in the next 24 months, with the rest expecting no change.

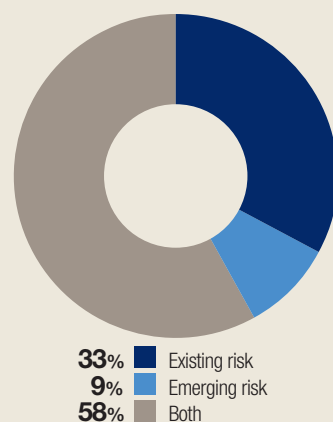
None of the respondents will be scaling down their use of scenario planning in the next two years.

“Only 37.5% tested for major failure of plant. Either this is seen as less important as IT systems breaches or failures, or not many respondents rely on manufacturing plants.”

The top two risk scenarios tested by respondents (networks/systems/power outage and cyber attack/data breach) reflect the increasing dependence on IT systems and the associated risks of this dependence. However, apart from these two and property damage – ranked among the handful of risks that the majority of respondents have tested for in the past year – there is no clear consensus on the important risks facing the industry.

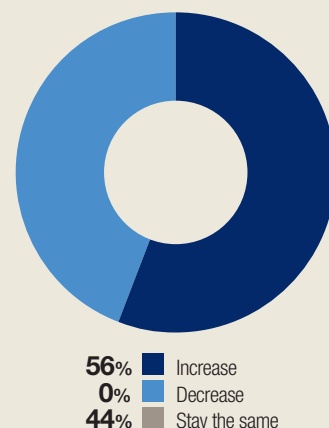
Only 37.5% tested for major failure of plant, suggesting two possibilities. Either this is seen as less important than IT

1 Do you mainly use scenarios to test



2 How many scenario tests do you conduct each year on average? 7

3 How will your use of scenario analysis change in the next 24 months?





systems breaches or failures, or not many respondents rely on manufacturing plants.

Meanwhile, given the significant increases in regional and global regulatory burdens, it seems surprising that only half of our respondents test for this type of failure.

### Influences

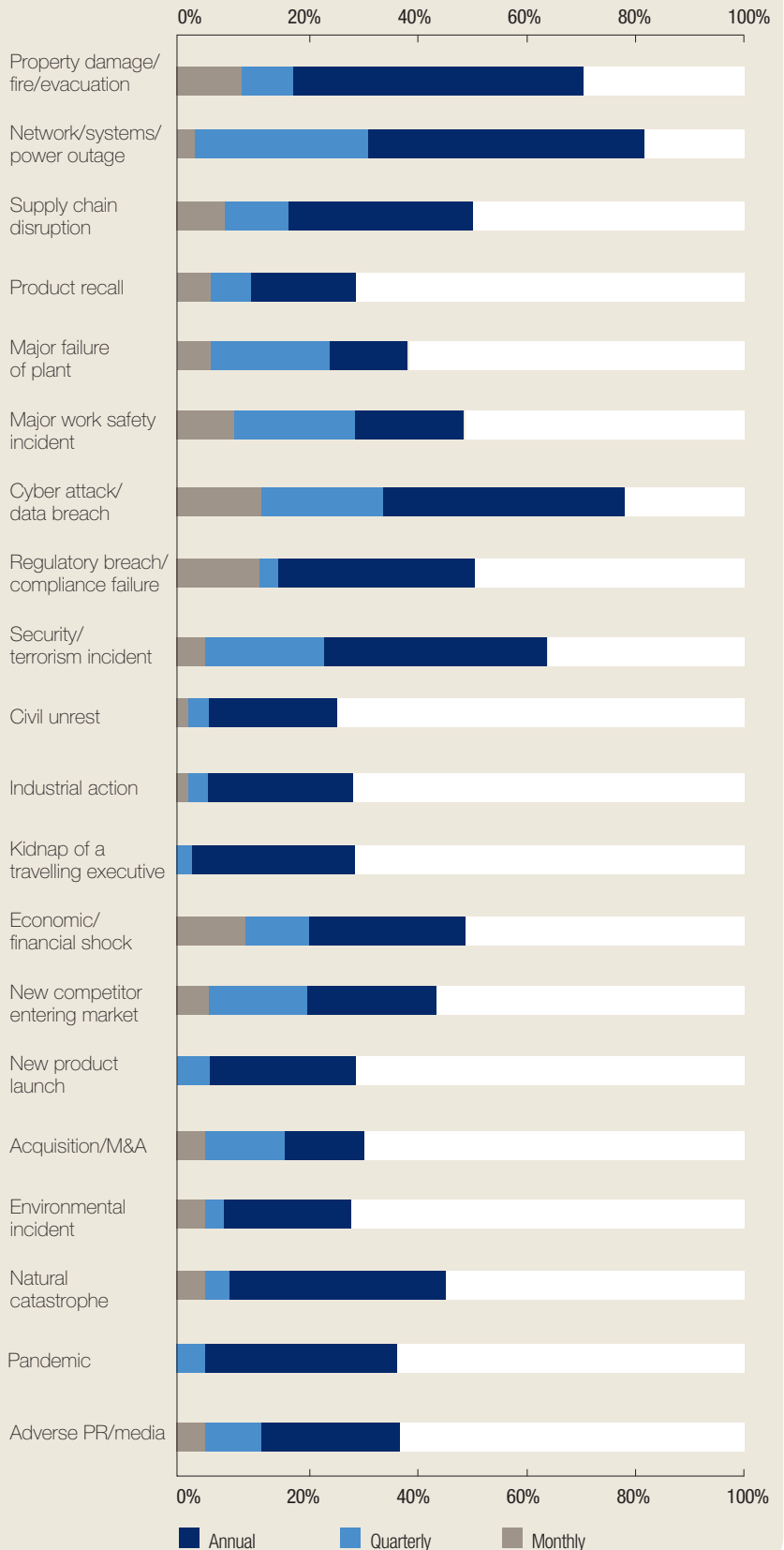
When asked to specify the principal factors influencing their choice of which scenarios to test, 79% of respondents opted for the risk register and emerging risk maps (for this and one other question, they could choose up to three answers).

Principal risk severity, impact and probability came next with 62%, followed by requests from the board, non-executive directors and any external stakeholders (55%). Once again, regulatory requests and compliance were lower down the rankings, with only 29% identifying this as a key area.

To a question about how lifelike these scenario tests are, 62% of respondents chose one primary event with multiple impacts. Cascading events and resulting impacts (where one event leads to another) and primarily one event and one impact were fairly close, scoring 17% and 14% respectively.

The testing of end-to-end business processes including suppliers is one of the least-used risk scenarios, according to our survey. Only 17% bother with this method, compared to the 40% of respondents who

**4** Which of the following risks have you tested using scenario analysis in the past 12 months and how often have you conducted tests?



Source: StrategicRISK Knowledge Survey 2017

## THE KNOWLEDGE

test segments of a business process, but more than one internal functional area or business line.

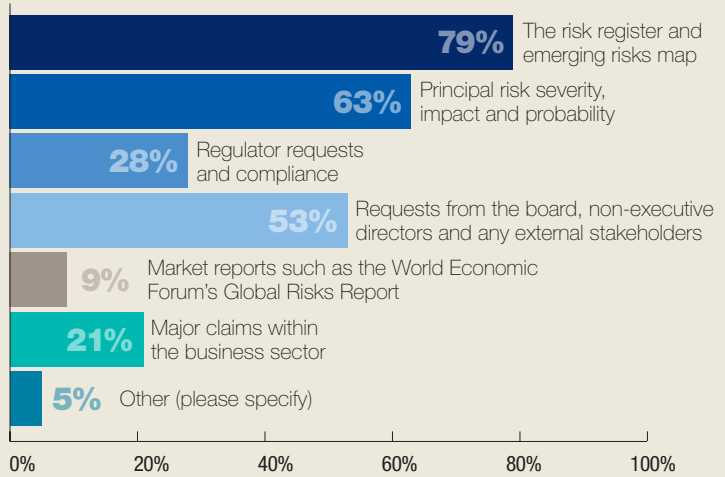
Almost half of our respondents use risk scenario workshops as a way of scenario planning, whereas only 10% use surveys of key stakeholders. About a third use risk scenarios integrated into business planning.

Just over a third of respondents benchmark their scenarios against some form of external loss data or industry-wide information. Is this because they don't care, or because the information is not readily available?

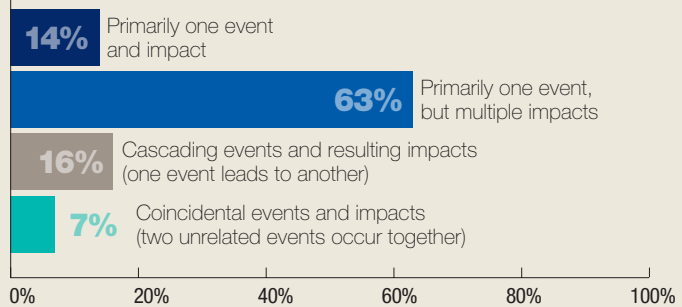
According to 63%, the main benefit of using scenario planning as a risk management tool was that it created a risk-aware culture across the business.



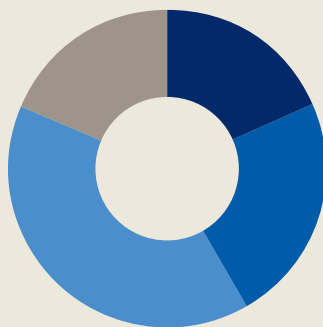
**5** What are the main factors influencing your choice of scenarios to test? (Choose up to three)



**6** How lifelike are MOST of your risk scenarios?

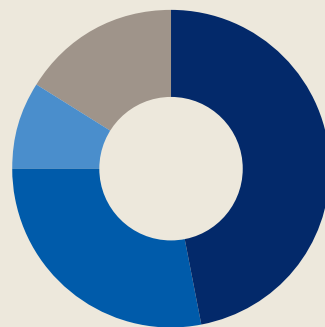


**7** Are most of your risk scenarios



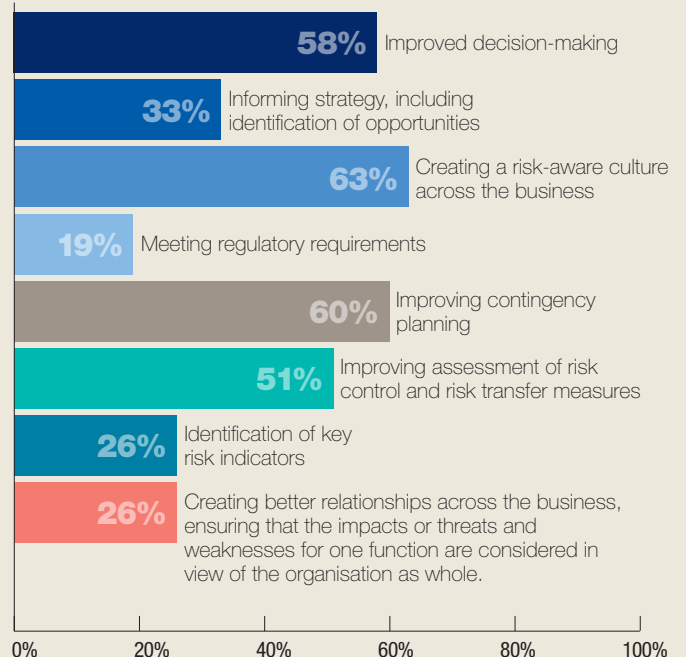
- 19% Testing an end-to-end business process, including suppliers
- 23% Testing an end-to-end business process, internal steps only
- 39% Testing segments of a business process, but more than one internal functional area or business line
- 19% Testing functional area or business line

**8** In what form do MOST of your scenarios take?



- 47% Risk scenario workshop
- 28% Risk scenarios integrated into business planning
- 9% Survey of key stakeholders
- 16% Other (please specify)

**9** What are the key business benefits of scenario planning? (Choose up to three)



## EXPERT VIEW

**MERVYN REA**, HEAD OF RISK ENGINEERING (AUSTRALIA & NZ), HEAD OF RE CUSTOMER MANAGEMENT, APAC. SENIOR RISK ENGINEER, ZURICH

# THE VALUE OF A HAZARD ANALYSIS

When a corporation experiences a real-life scenario that's tangible, there is a huge opportunity to learn from that experience, to review what precisely happened, to do a root-cause analysis and determine what the triggers were that made that scenario occur. They can then revise and review whatever risk controls they thought were adequate at the time and decide whether they need to improve them.

It is said that there's nothing better than learning from your mistakes, although real-life disasters are not necessarily mistakes, so in this case it about learning from actual scenarios. When these real-life experiences occur, there is a great opportunity to help ensure that the same scenario does not reoccur, or if it does, at least without the same disastrous impact.

At Zurich, we have developed a method called Zurich Hazard Analysis (ZHA). We can use the ZHA approach to look at real-life scenarios that have occurred in the past; and also hypothetical scenarios, some of which are real and potentially tangible, but have not yet occurred.

While most firms tend to plot hazards on a five-by-five matrix, we choose six-by-four to prevent 'sitting on the fence'. Once we've identified all of those scenarios, hazards, triggers and the effect of those and plotted them on the matrix, we then work with the customer to determine what their line of tolerance would be. That tolerance is then plotted on a matrix, and anything located above that line of tolerance, they are essentially risks that nobody is prepared to accept.

Once we have identified these risks, they need to be 'treated' (in other words, current controls improved or modified). Next we revise what that hazard would look like if those risk controls or risk treatments were in effect, plotting the lesser hazard on the same matrix. Hopefully, using ZHA we can bring those hazards down below that line of tolerance and keep reducing those hazards until we achieve an acceptable

outcome, so it becomes a risk that is digestible or tolerable.

By going through that process for a number of scenarios, we can develop a hazard catalogue: a range of hazards associated with that scenario, the various triggers that would cause it, and for those hazards that are unacceptable, we have a risk improvement action list, which then the customer can implement.

When it comes to technological innovations, if there are efficiencies to be gained from using smarter technology, maybe more predictive technology, then we will always look to incorporate that into our methodologies. But a risk for one company is not necessarily exactly the same for another company, so we find that the personal engagement and involvement

“ Often when we use this approach with customers, the outcomes show they hadn't fully appreciated the magnitude of the risk to their business.”

**Mervyn Rea, Zurich**

of our experienced people is what makes ZHA most successful.

One of the things we've discovered in using ZHA is that quite often, there are scenarios and risks that businesses are experiencing or already aware of. Often, the triggers for those hazards are staring them in the face. Many times, they've become almost accustomed to them or they haven't fully understood the ramifications should an incident occur.

The ZHA methodology leaves no stone unturned. So often we find when we use this approach with customers, the outcomes produced show they hadn't fully appreciated or understood the magnitude of, or the full impact of, the risk to their business, particularly with brand and reputation. Some customers raise their eyebrows because they hadn't fully

comprehended the maximum outcome that could occur. In some cases, they thought their existing risk management controls were adequate, but with ZHA they soon realise that existing controls do not bring that hazard below that line of tolerance.

Because of this, they're more sharply focused on introducing new controls, or improving existing controls and measures so that they can reduce the outcome of that risk to something that is more tolerable or acceptable to their business.

We find that engagement with our customers becomes stronger following a ZHA exercise, as we become their trusted adviser. In some cases, we have customers who have become so familiar with the methodology that we actually provide them with the training so they can facilitate their own ZHAs internally.

In general, society tends to assume that large global or national organisations are secure when it comes to cyber security. Indeed, people are often critical when they hear about a cyber breach of some kind. At Zurich, we've been slowly developing an approach in Australia to use a ZHA specifically for cyber risks. All of our risk engineers are trained facilitators of ZHA, and with a Cyber ZHA, we bring a further subject matter expert into the room – a penetration tester.

The real success of ZHA is that we get the right experts in the room from the customer, across a broad range of disciplines. We get the right decision-makers and knowledgeable people that are closely related to whatever scenario or scope is being addressed in the ZHA.



► THE STRATEGY

# Testing conditions

While planning a scenario, executives must first determine which factors to consider.

Incidents such as natural catastrophes, industrial accidents, social or political unrest and upheaval can lead to significant losses for businesses around the world. Stress-testing how your organisation's policy could respond to possible loss scenarios can test how the insured's policies should respond and help avoid costly delays when the worst happens.

Nearly half of risk managers could benefit from being better prepared for a major or complex claim by conducting scenario analysis, according to research by UK-based Echelon Claims Consultants, a subsidiary of JLT Specialty.

While 65% said they had prepared a claims plan in case of a major loss, only 41% had carried out any form of loss scenario planning to test these plans and confirm that their insurance coverages would respond as expected.

"Companies that get caught up in major incidents are often shocked by the magnitude of the losses, and then the sheer complexity of the insurance claims process that follows," says Candy Holland, managing director at Echelon.

"Many companies underestimate the resources needed to deal with claims. This can lead to costly delays and, potentially, shortfalls in the claim settlement."

She adds: "It's encouraging to see that the majority of risk managers have carried out some form of planning for a major incident, but it concerns me that nearly two-thirds haven't actually stress-tested these plans."

"Carrying out a loss scenario exercise is a good way to challenge any existing plans, as well as engage with insurers at an early stage to ensure they have the correct cover in place for the needs of their business."

## Avoiding underinsurance

One coverage that is often looked at closely during scenario planning exercises is business interruption (BI). About a third of insurance buyers set their maximum BI indemnity period at 12 months, but considering how long a business could be out of action, this is often deemed to be inadequate. Indeed, just 17% of risk managers are "extremely confident" their BI values and limits set are adequate, a survey



by the Risk Management Society (RIMS) found.

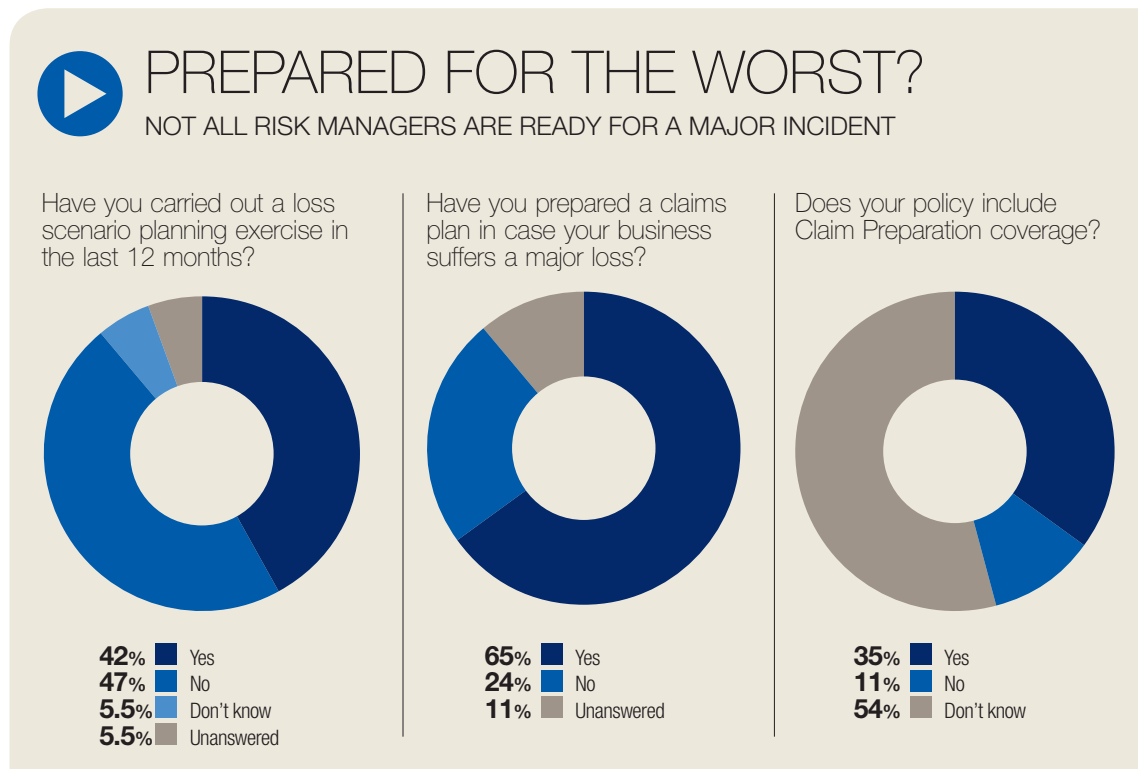
"If you burn down your factory with all the machinery in it, my experience is that it is highly unlikely that you will get the business back up and running within a year," says Geoff Piggot, CEO of Crawford GTS. "You've got to clear away the debris, get people into

When you bring in adjusters, brokers and insurers that have seen a lot of losses in the past, they can bring a sort of a realism to the business contingency plan that perhaps it doesn't have."

**Geoff Piggot**  
CEO, Crawford GTS

redesign, get planning consent, you've got to source machinery etc, and the insured can underestimate how long all of this will take them.

"And then, even if you get back up and running and you're producing, it's quite likely that you won't get all your





customers back immediately. It will take you time to win back your customers and get you back to a level of turnover that you were at prior to the loss. So quite often we find, if you do this scenario planning, the insured reaches the conclusion that 12 months' BI is a bit optimistic and that realistically they may need 24 months."

Among the 40% of risk managers who had experienced a BI loss during the past five years, nearly 60% said their main challenge was quantifying the loss. Other notable issues included coverage not responding, disagreements between adjusters and insureds and a lack of understanding by the insurers' representatives of the insureds' business/impact due to loss.

Additional problems included personality issues, an uncooperative adjuster/forensic accountant, suspension period issues and a lack of direction when preparing a claim. Scenario analysis can help avoid issues such as these as it brings together all the parties that are likely to be involved in a complex claim before the loss actually occurs.

"A lot of businesses do have a business continuity plan. But what can happen is that it can almost be written in a bit of a vacuum," explains Piggot.

"When you bring in adjusters, brokers and insurers that have seen a lot of losses in the past, they can bring a sort of a realism to the business contingency plan that perhaps

it doesn't have. Then you can take a practical approach to determining exactly how the policy is going to respond to a particular type of claim.

"For example, you or the business may eventually decide that you need additional cost of working coverage. This kind of coverage is quite often used for things that are slightly

more difficult to put a value on, such as marketing and promotion. And insurers will usually quite happily spend 50 pence to save a pound in lost gross profit."

Before he moved into loss adjusting, Piggot worked in insurance and reinsurance, offering him a unique perspective into how scenario planning can assist all parties to a claim.

"As a re/insurer, you actually end up with a better risk following scenario analysis, because in the event of a loss, you will have looked at the coverages, at the premises, and will have made some recommendations. And therefore if something bad does happen, you're likely to have a financially smaller loss."



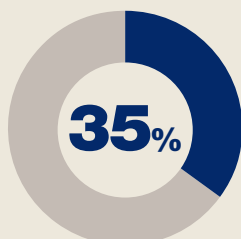
Please indicate on the scale your confidence in the values declared/limits set for your BI cover:



### BIG NUMBERS

**41%**

Proportion of risk managers who have carried out pre-loss scenario planning



Proportion of insureds who have just 12 months of BI coverage

**17%**

Proportion of risk managers who are "extremely confident" their BI values and limits are adequate

Source: RIMS and Echelon

► THE EXPERTS

# Look at it this way

How effective is scenario analysis in reality? Three respected figures from the Asia-Pacific risk community tell us how they put the theory to practical use.

JEFFREY YEO,  
ENTERPRISE RISK MANAGER,  
SINGAPORE POOLS



## How can scenario analysis be used to enhance risk management?

This is about identifying potential issues affecting the operations of business units and, through risk management, designing practical and realistic mitigating measures to handle them – an anticipative and proactive approach to pre-empt what might and could happen.

The first thing that comes to mind when I think about scenario analysis is ‘prediction’, but prediction with limited information on hand. It is about accepting and embracing uncertainty with limited certainty of information.

The identification of such scenarios could be done through meetings or workshops with key stakeholders and domain owners. These will then be presented to senior management for approval.

The testing of such scenarios is akin to business continuity planning. Ideally, the identified risks should be tested at least once a year and the assessment be reviewed from time to time, depending on the nature of the industry and the overall fluidity of the business environments.

## What are the key benefits of using scenario analysis?

Scenario analysis itself is a management tool to enhance decision-making and strengthen risk management. It is a systematic process of obtaining insights and inputs from domain

“The first thing that comes to mind when I think about scenario analysis is ‘prediction’, but prediction with limited information on hand.”

**Jeffrey Yeo**  
Enterprise risk manager,  
Singapore Pools

experts and risk managers to derive reasonable assessments of the likelihood and impact of possible scenarios that could occur on business operations.

A proper and robust scenario analysis boils down to asking the right questions and preparing for the unexpected.

## What are the key challenges risk managers face in developing scenarios?

One challenge is the identification of risks that are relevant to the business. Scenario analysis helps to narrow and set the essential boundaries to segregate what is relevant against what is not.

There are two ways of identifying risk scenarios: (a) from the perspectives of the business’s objectives (specific) and (b) generic identification of what can go wrong (general). Both approaches are complementary and must be used simultaneously.

The generic approach is an easier place to start and creates a basket of possible scenarios. From the angle of business objectives, the identified scenarios can then be narrowed down to those that are relevant and more importantly, realistic.

As a rule of thumb, ask:

- What are the objectives of the scenario identification and analysis exercise?
- What is the strategy or decision that my scenario analysis is going to influence?
- Why has this scenario been chosen?
- Who will be the stakeholders I need to work with as a risk manager?

The components of a risk scenario are:

- Event (operation failure, regulatory changes, climate changes, pandemic outbreak, etc)
- Threat (staff oversights, terrorism, etc)
- Stakeholders (department heads, process owners, external vendors, etc)
- Asset/resource affected (processes, infrastructure, staff, etc)
- Time factor (possible duration of downtime, etc)

With the identification done, the next step will be to determine the frequency of these scenarios occurring and the estimates of the business impacts in the event that these scenarios become a reality.

## How should risk managers communicate and use the results of each scenario?

As risk managers, we all know and appreciate the importance of cascading risk management initiatives and creating a risk-awareness culture within our community; likewise for the outcomes of scenario testing.

The stakeholders who participated in the process may be aware, but the next in line are the operations managers. Staff who are actively involved in executing the day-to-day business operations also need to be brought up to speed.

Communication channels differ among organisations and companies. Nonetheless, those who may not be directly involved in the scenario planning and identification processes also need to be aware that such an exercise did happen as part of creating risk awareness within the business entity.

In addition, for those who have actively participated in the processes, they would also need to have the skillsets and knowledge of performing assessment treatment and ultimately monitoring the likelihood of such scenarios.

Finally, but importantly, senior management awareness and assurance need to be communicated at meetings – the assurance being that such scenarios are being monitored and mitigating measures are available.

Risk managers will need to work closely with relevant stakeholders in the monitoring and review of such cases and to the senior management, in their strategic planning capacities, all of these scenarios will play a part in the game plan.



PIERRE BALDACCHINO,  
RISK ANZ, BAYER  
AUSTRALIA LIMITED

### How can scenario analysis be used to enhance risk management?

Incorporating a well-executed scenario analysis package into an organisation's overarching enterprise risk management program turns the all-too-common and often mundane risk profiling and reporting process into a more dynamic risk management approach.

It moves an organisation away from simply looking at bubbles on a two-dimensional heat map to being confronted by and understanding the potential impact (both positive and negative) of a risk event.

Ideally, scenario analysis should be incorporated during both the standardised risk profiling cadence (performed with key executives) and when significant change activity occurs. Often the simplest and most effective way to deploy a scenario analysis program is to ask the board or executive situational questions: "We're approaching the end of our three-year strategy and we've not delivered on our goals. Why?" This helps target realistic problems or opportunities to tackle in detail and provides some level of boundary to an approach that can quite easily become broad and adventurous.

### What are the key challenges risk managers face in developing scenarios and how can they address these?

Often the problem with scenario analysis is that the scenarios become too broad and stretch beyond what management would deem to be a realistic or plausible event, i.e the likelihood of the scenario is considered to be extremely rare.

Risk managers need to balance not only the likelihood and consequence of scenarios but also consider the third element of speed (or velocity) with which a scenario can impact an organisation.

Again, asking situational questions and co-developing a scenario with executives during these sessions will lead to the natural development of plausible scenarios.

Utilising case studies, topical events or emerging trends that have impacted other organisations in your region or market are also beneficial to trigger discussion – again, it adds that element of 'realism' that turns the discussion into something that could realistically impact strategy.

### How should risk managers communicate and use the results of each scenario?

The results of scenario analysis need to be measured against an organisation's risk appetite statement – if the impact of the scenario is material enough to deviate from what is acceptable, focus needs to be placed on potential treatment plans.

Where scenario analysis programs are embedded effectively, the results should seamlessly integrate into the overarching critical risk profile for the organisation.

SUSIE JONES,  
HEAD OF CYBER SECURITY  
BUSINESS SERVICES,  
INFORMATION SECURITY  
OFFICE, AUSTRALIA POST

### How can scenario analysis be used to enhance risk management?

If I focus on cyber security, the vast majority of incidents involve human error, and one of the most common methods of falling victim to a cyber attack is still through clicking on a malicious link in an email. Businesses can help train their staff on what to look out for and avoid by



Running regular scenario tests (or phishing email simulations) will deliver immediate training to any staff who click on the link in the test email."

**Susie Jones**  
Head of cyber security,  
Australia Post

running regular scenario tests (or phishing email simulations) that deliver immediate training to any staff who click on the link in the test email.

### What are the key benefits of using scenario analysis in risk management?

The benefits of phishing email simulations are largely twofold. You provide any staff who click on the link with immediate training, thus reducing the risk that they will click on a 'real' malicious link, as well as gather data on the behaviour of your staff that can help you to understand where else you may need to focus your training efforts. If you run an invoice-themed simulation and 30% of your payments or procurement team click the link, then you know you need to focus on those areas. If only 5% click on the link, perhaps you can move on to other parts of your business.

### What are the key challenges risk managers face in developing scenarios?

There are many vendors offering easy-to-use programs these days so setting up the scenarios is less of a problem, but depending on what programs you use, much of the data analysis can still be very manual, so it can take a lot of man-hours to get the insights you are looking for. I recommend closely considering this when choosing who to partner with for simulation testing.

### How should risk managers communicate and use the results of each scenario?

Phishing email scenarios provide data that everyone understands, so I recommend spreading the word far and wide. Cyber security is still a topic that many hide away from, so risk managers should use these kinds of insights as much as possible to push for a more secure business.

► THE INTERVIEW

# ‘We’re picking up strange things and we need to talk’

With the help of various doodles, former OECD strategist Angela Wilkinson explains the concepts behind scenario planning in plain English.

If *The Knowledge* learned one thing during this interview, it is that Angela Wilkinson likes to draw. Strange as that may seem – it’s not something one automatically associates with a physicist, 30-year risk and uncertainty veteran and former strategist for the Organisation for Economic Co-operation and Development – she can take a complex concept like scenario planning and turn it into an easily understood doodle.

“When we think we are being overwhelmed by the anxiety of uncertainty, the first thing we need to do is just draw a box. We say, ‘Look, that’s our familiar, comfortable box. That’s got all the things we know in that box.’ Then let’s draw another box and say, ‘What are the things we don’t know?’ and let’s start putting them in that box. Don’t make it too big a box; just make it different. Then draw another box and find another set of things that are different there. And there you have scenario planning.”

Seems simple, right? Wilkinson thinks so. “Scenarios aren’t designed to make you think about everything you can’t manage. They’re designed to give you a set of frames, which are different enough that you don’t fall into the forecasting trap when things are changing. It is not about developing a million scenarios but rather about developing two or three things that are useful and challenging that you can use to test and contest the assumptions you’ve built into your risk assessment.”

Or to put it in another way: “It is not a risk manager’s job to boil the ocean to find gold.” Risk managers have to scan the horizon, but do so intelligently, she says, as the ultimate decision-maker will be looking to make a decision with immediate effect.

“What we want to know is, what are the assumptions the decision-maker is betting



“When you get signals that people are defaulting on their mortgages more than they’ve ever defaulted in history, don’t dismiss it as a noise aberration. Ask yourself, what are we learning?”

**Angela Wilkinson**  
Risk and uncertainty expert

the shop on? We don’t want to know all their assumptions and all their theories about everything. We just want to know, what are the critical assumptions built into this decision that we’re about to make about the future? And importantly, are those assumptions valid?”

Invalidation of models is one of the biggest challenges facing risk managers, particularly when a freshly implemented model is showing signals of doubt early on. The brain’s tendency to dismiss signals that do not fit with preconceived ideas is something risk managers must fight.

Referencing US subprime mortgages, Wilkinson says: “When you get signals that people are defaulting on their mortgages more than they’ve ever defaulted in history, don’t dismiss it as a noise aberration. Ask yourself, what are we learning? Why will this invalidate our model? To do that, you have to start looking for signals of things

that you don’t want to see. This is the hard part. Find a space to have a conversation with people who are relying on you to give them the answer; to say, ‘We’re picking up strange things. We need to have a conversation with you about this.’”

She says most organisations don’t have the bandwidth needed for this. “It’s like a huge information production factory. You’ve got to get the product to perfection, give it to the marketers and out it goes.” As soon as imperfection is acknowledged, the degree of uncertainty is extrapolated.

Paradoxically, there is a case to be made that too much data is partly responsible for this uncertainty. “The way we’re organised as a society is based on the more data you have, the less uncertainty you’ll have. We’re living in a world where we’re finding the more data you have, not necessarily the less uncertainty you have. Analysing and understanding that data is the hard part.”

While uncertainty does have a place in scenario planning, because it gives scope and breadth, Wilkinson says caution should prevail. “Think about how the Wright brothers did their risk assessment. They built a plane, hopped in and hoped they didn’t die if the wings fell off. That is called learning as you go.” We still build planes, fill them with passengers and hope that they fly, she adds, but we also use wind tunnels and test the parts in advance.

The difference between a conventional risk analysis (like the Wright brothers’ first flight) and a scenario-based risk analysis is often confused, she says. The former might use scenarios, but the models have a baseline projection with variations. There is quantifiable uncertainty and from that, risk managers will usually derive three scenarios – high, medium and low-risk.

“In scenario planning, we are saying, ‘All the straight-line projections could be wrong.’ We are not just interested in whether the impact will just be higher or lower, we’re interested in ‘how will it be different?’ and ‘will this situation occur at all?’” says Wilkinson. “In scenario planning, we deliberately look beyond the usual evidence base that’s used to make the risk analysis and we ask, ‘what if?’ questions.”

Scenario planning uses different assumptions from conventional risk models. The traditional risk analysis model has a whole series of assumptions built into it,

“Think about how the Wright brothers did their risk assessment. They built a plane, hopped in and hoped they didn’t die if the wings fell off. That is called learning as you go.”

**Angela Wilkinson**

Risk and uncertainty expert

and their scenarios are the uncertainties of those assumptions. But in scenario planning, it is assumed that model works only under certain conditions, and the scenarios noted are the conditions under which the model might fail. In other words, don’t look at the uncertainties in the model; look at the uncertainties of the model itself.

“Risk managers spend their time taming uncertainty. Think of them as courageous people who use numbers to tame uncertainty. Now let’s look at scenario planning: a conventional risk manager thinks of uncertainty like an ice cream cone.

“When you’re a risk manager, you’re standing in the present and in front of you, uncertainty is opening up and you’re trying to work out how you calculate the future and keep it within some definable zone. It’s like a cone going out in the future, and your job is to try and make that cone as small as possible, but not so small that it’s a single point, because you know there is uncertainty. That’s your job as a risk manager,” says Wilkinson.

Now consider the cone from a scenario planning perspective. “That cone assumes that we know where we stand already, and we don’t. Often in normal or emerging situations, we’re not sure what the starting point is, so we have to be a little bit more flexible about those framing assumptions.”

Could anything be learnt during the process of using these types of scenario assessments? “No, because risk assessment isn’t the same as an innovation frame. In an

## Brexit’s four distinct possibilities

Brexit can be easily classed in an emerging risk frame but that is where the simplicity ends, says Wilkinson. “It is impossible to calculate the exact nature of the risk on the basis of a repetition of history as there’s no precedent, so instead, use of scenario planning comes into the frame.” Finding a way to organise the uncertainties is key. Below is one way of scenario planning for Brexit.

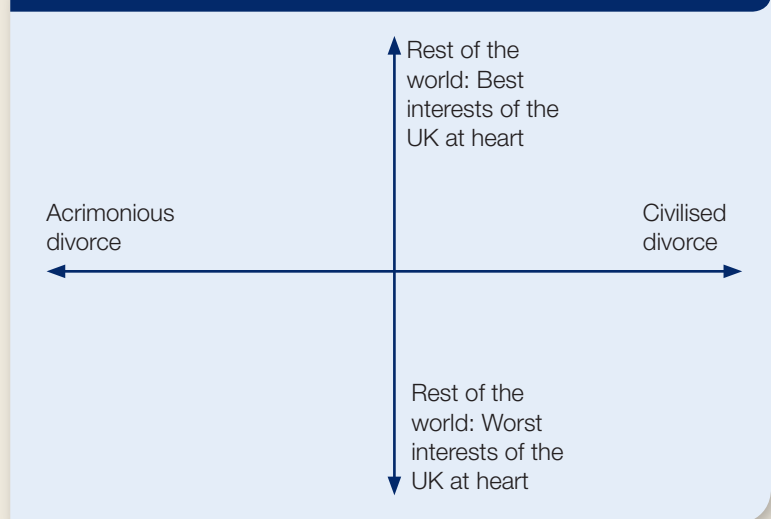
“This gives us four different scenarios. Now ask yourself: are you in the scenario where it’s civilised divorce and the rest of the world’s behaving themselves? Or are you in the scenario where it’s uncivilised divorce, and the rest of the world is going to make this as difficult as possible?”

- We say, “Look, that’s our familiar comfortable box. That’s got all the things we know in that box.” Then let’s draw another box

and say, “What are the things we don’t know?” And let’s start putting them in that box. Let’s not make it too big a box, let’s just make it different. Then let’s draw another box and find another set of things that are different there, and then we’ve got scenarios.

- Scenarios aren’t designed to make you think about everything you can’t manage. They’re designed to give you a set of frames, which are different enough that you don’t fall into the forecasting trap when things are changing, in risk management. So it’s not about developing a million scenarios, it’s about developing two or three things that are useful and challenging, and you can use to test and contest the assumptions you’ve built into your risk assessment.

### ▶ PLANNING FOR INDEPENDENCE



innovation frame, we’re deliberately learning as we go. We’re prototyping fast and learning from our mistakes. If you want to learn as you go, use an innovation frame.

“With a risk frame, we are asking questions about how we can minimise losses and minimise any downsides. We know

there’s an upside, but how do we get rid of the downside? In the risk frame, when we think we’re being overwhelmed by uncertainty, because uncertainty makes us anxious, the first thing we need to do is just draw a box.” And just like that, we are back to boxes.

# NOW YOU CAN KEEP AN EYE ON YOUR RISKS FROM ONE PLACE.

Protecting the business you love is easier when you have a clear view of what might affect it. My Zurich is an online portal that gives you 24/7 access to real-time claims data, the status of your policies and wordings, including benchmarking for risk engineering data, in a transparent way.

**FIND OUT MORE AT**  
[zurich.com/my-zurich](https://zurich.com/my-zurich)



**ZURICH INSURANCE.  
FOR THOSE WHO TRULY LOVE THEIR BUSINESS.**



**ZURICH<sup>®</sup>**

This is a general description of insurance products and services and does not represent or alter any insurance policy. Such products and services may be made available to qualified customers through appropriately registered companies of the Zurich Insurance Group in the Asia Pacific region, including: in each of Hong Kong, Singapore and Japan; Zurich Insurance Company Ltd (a company incorporated in Switzerland) which is registered in each of these territories; for corporate life solutions in Hong Kong, Zurich Life Insurance Company Ltd; in Malaysia, Zurich Insurance Malaysia Berhad; in China, Zurich General Insurance company (China) Limited; and in Australia, Zurich Australian Insurance Limited ABN 13 000 296 640.