

Integrating Emerging Risk: an alternative perspective

Integrating emerging risk into risk management frameworks and capital models is challenging for insurance companies. Buu Truong and Gemma Gregson investigate whether analysing cause, rather than effect, can help overcome some of the difficulties.

Over decades of experimentation and experiences, insurers have learnt how to successfully manage a wide variety of risks that they face in their day-to-day business. However, the world never stops moving and the risks keep evolving, presenting new challenges to the industry. Among today's problems is how to deal with probably the broadest risk category of all: emerging risk.

There appear to be many similarities between operational risk and emerging risk, such as a lack of information and the heavy reliance on expert judgement. So perhaps we ought to turn to operational risk to guide us in establishing a framework for the management of emerging risk. In writing this article, we have general insurers, rather than life insurers, in mind.

Approaches to operational risk differ between companies, but many focus on using a range of scenarios to generate a broad understanding of the breadth of operational risk. Scenario analysis provides a logical framework for a qualitative discussion and by relating the risk to real-world examples, it makes it easy to understand.

Assuming that there is a robust framework in place for identifying emerging risk scenarios, they can be analysed in the same way as operational risk scenarios. While there is nothing particularly new in using scenario analysis for emerging risk, this article considers the benefits of integrating emerging risk processes with those of operational risk.

Cause versus effect

Treating emerging risk like operational risk is a start, but there are still some hurdles to overcome. One such issue is that it can be difficult to know if all emerging risks have been considered, not helped by the fact that the emerging risk list is somewhat of a moving target as some emerging risks become known risks and therefore drop off the list, while others come in to replace them.

In addition, discussions centred on particular scenarios are not always the most productive use of time in a resource-constrained business world.

While traditional scenario analysis has served the industry well in considering operational risk, perhaps what is ultimately required for both operational and emerging risk is a framework that augments an understanding of events with an understanding of risk drivers.

Here the PESTLE framework can come in handy. PESTLE stands for Political, Economic, Sociological, Technological, Legislative and Environmental and provides a way of thinking about the root causes of a particular risk.

This driver-based work lays the foundations for integrating scenario analysis with internal models. Models can't easily adapt or link to specific scenarios, but, as we discuss later, connections to models can be made through the process of going back to root drivers.

The starting point of the framework would still be scenario-based, but rather than just asking how the scenario would impact the business, the question would be around the drivers to the scenario and whether they are political, economic, social and so on. Each scenario could be ranked qualitatively in the PESTLE framework according to how significant a driving force each element is considered to be to the scenario.

This is best illustrated by means of an example. For the sake of argument, let's assume that cyber risk is an emerging risk. A PESTLE rank of an emerging cyber risk scenario could look something like figure 1. It is highly technology driven, to some extent social, but less affected by political and economic conditions, legislation and the environment.

Figure 1: PESTLE ranking of a cyber risk scenario

P	E	S	T	L	E
Low	Low	Medium	High	Low	Low

The relevance of emerging risk today

The next step would be to consider a scenario in terms of its contribution to each of insurance, market, credit and operational risk. The results could be presented as in figure 2 which shows what the analysis could look like for our cyber risk scenario.

At this point, it is helpful to think about the time horizon of emerging risk. When we consider the word emerging, we think of something that is just beginning to exist. As such, it can be easy to view an emerging risk as one that will impact a business in the future and that will not have an effect on the business today.

That doesn't feel right. Emerging risk does affect our current risk profile and does exist on our current balance sheets. An extension of this is that emerging risk should also be included within our capital assessments. The difficulty is in understanding to what extent emerging risk is relevant now.

With this in mind, it can be helpful to view emerging risk both in terms of the impact on the balance sheet today and in terms of the potential impact in the future.

In the short term, risks affecting the business are largely unintended losses on typical insurance products. In our cyber risk example, business interruption cover may inadvertently open up cover for interruption from a cyber attack if not explicitly excluded.

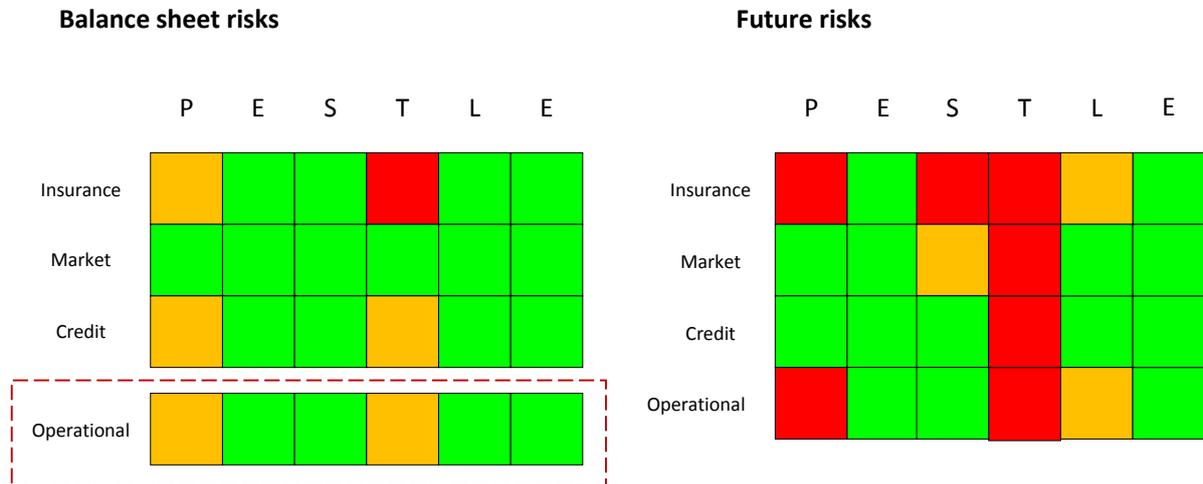
Over the longer term, the risks are more strategic; they have the ability to affect the overall business model. Continuing our example, emerging cyber risks such as portable working and data security change the way a business operates, while the potential for insurance to be bought through social media sites can impact how an insurer can attract and retain business.

Figure 2: Contribution of a cyber risk scenario to balance sheet risks and future risks

	Balance Sheet Risks	Future Risks
Insurance	High	High
Market	Low	Low
Credit	Low	Low
Operational	Low	Medium

Once the analysis underlying figures 1 and 2 has been repeated for all scenarios, the final step would be to consider those scenarios that significantly influence the risk categories and work backwards to the PESTLE framework to ascertain the extent to which each element of PESTLE gave rise to that high ranking. The results of the analysis could be illustrated in a diagram like that in figure 3 which could be produced both for each individual scenario and for all scenarios combined.

Figure 3: Heat map of importance for all scenarios combined for a fictional company



Green represents a driver that is of low significance to a particular risk category, orange represents medium significance and red high. Looking at insurance risk, the chart shows that political drivers have medium impact on the balance sheet today in our fictional company but are of high importance in the future. Contrast this with the impact of social drivers on insurance risk, the influence of which are unlikely to be significantly felt until some point in the future.

When interpreting figure 3, it is important to realise that it is the extent to which the drivers are important for each of insurance, market, credit and operational risk that is of concern, rather than the perceived relative materiality of the link.

For example, while economic drivers are highly likely to drive market risk on an overall level, in terms of considering emerging risk, it may be that such a relationship between economic drivers and market risk is not relevant to the company.

The purpose of this exercise is to understand which drivers are important and where they may impact the business both now and in the future. Although the actual figures that come out of this prioritisation exercise may not be robust enough for reporting purposes, the value in doing the exercise itself should not be underestimated.

Casting an eye down the future risk columns, we see a block of green against environmental issues and a sea of red against technological. This information could be used to prioritise technological risks over environmental ones.

We are not saying that environmental risks ought to be ignored, but that in this example, the rewards of making strategic business decisions having regard to technological risks may be greater than spending resources thinking about environmental emerging risk scenarios.

Once the information has been gleaned from the process, it ought to be regarded like any other element in a risk management framework; not as something that is set in stone, but as something that can be used to aid decision making and as part of a dynamic process that can be revised should circumstances warrant it.

Linking to capital models

The dashed box in figure 3 represents the current remit of some operational risk teams who work to understand drivers behind operational risk scenarios. These drivers can form the base of correlation assumptions with other risks in the model.

It is in this direction that such a PESTLE analysis for emerging risk also extends. Companies already employing these methods for operational risk could gain efficiencies by incorporating emerging risk into the analysis for balance sheet risks.

Despite often being the reason for business failure, emerging risk typically has to fight for scarce risk management resource. Integrating emerging risk with other processes would go some way to help win the battle.

Solvency II requires material quantifiable risks to be included in the solvency capital requirement (SCR). Although it can be credibly argued that due to the slow emergence of emerging risk, the one-year horizon of the SCR is short enough to plead immateriality, ultimate time horizons are different. It is not uncommon for the ultimate horizon of an employer liability policy to include the potential for new latent claims to emerge, yet when it comes to other emerging risks, they are not generally linked to modelled ultimate variability.

A method of incorporating hard-to-quantify risks into capital models that is already employed by some companies for operational risk, is to consider the causal relationship between the risk scenarios and other risk types that are more easily quantified such as insurance, market and credit risk.

This relationship can be formalised through a set of indices which can then be used as modifiers to existing models. By using PESTLE to go back to root causes, it enables a link to be created between emerging and operational risk and capital models.

Each to their own

While the intricacies of risk management systems and capital requirements are unique to each business, considering the causes of risk and the timeframes over which each risk manifests itself could provide most general insurance businesses with a solid foundation on which to base decisions.

Any approach needs to stand up to both board and regulator scrutiny and while we are not suggesting that this is the perfect solution, we do hope that it will provide some ideas upon which to ponder.

Operational risk frameworks weren't built overnight. They were designed, created and modified over a number of years. Indeed, they are still being fine-tuned. There is still a long way to go before emerging risk is firmly embedded into risk frameworks, but it is never too early to start doing so.

Buu Truong is managing director of Insight Risk Consulting. Gemma Gregson is a senior consultant at Insight Risk Consulting. Email: buu.truong@insightriskconsulting.co.uk

