SPONSORED FEATURE

modelling risk scenarios

Operational risk modelling – finally?

The recent changes in regulation, in particular the Basel Committee's standardised measurement approach (SMA), are an opportunity to escape two misconceptions regarding operational risk – that it is not exposure-based and that extreme losses can be extrapolated from recurring losses, says Patrick Naim, president of Elseware

Operational risk is exposure-based

A couple of years ago, I was working with a client on a mis-selling scenario, which he proposed calling 'unexpected payments to customers'. This is a good illustration of the conception among operational risk practitioners in the financial industry, namely that operational risk is a sort of *deus ex machina* – very difficult, if not impossible, to predict or quantify.

Patrick Naim

This idea is rooted in a very simple misconception: operational risk is not considered an exposure-based risk. When businesses miss this dimension, they can be overwhelmed by the variety of events, which can seem difficult to identify and to structure. In addition, they are likely to mix up hazards, causes and events.

But, if one thinks about operational risk with a fresh mind, one will find that it is in fact very clearly exposure-based. Working with employees exposes a firm to fraud; working with traders exposes a firm to rogue trading; selling products exposes a firm to mis-selling; having competitors exposes a firm to cartels; and operating in buildings exposes a firm to natural disasters or terrorist attack. When looked at this way, no single operational risk is not exposure-based.

The single difference is that exposure is not a dollar amount, whereas exposure to credit risk and to market risk is a money amount. One lends a certain amount or takes a position, and this amount of money is exposed to a risk of default or to the volatility of the markets. This 'money' exposure may have hidden from banks the true definition of 'exposure at risk' – that it is a resource. A firm combines resources to achieve its objectives and any event that may harm a key resource will endanger the achievement of objectives: this is the definition of risk. In the case of banks, customers' money is certainly a resource. But employees, products, suppliers, and so on, are also resources, and these resources are exposed to operational risk.

The exposure is the number of objects that may be hit by a risk event, and other industries have identified this notion. In airline safety, for example, the exposure is the number of flights. Each time a plane takes off, it is exposed to a risk. The exposure in this case is certainly not a dollar amount, nor the number of passenger miles, nor the number of aircraft. A plane on the ground is not exposed to the risk of an accident.

A tsunami is not an unexpectedly big wave

The second misconception concerns potential loss forecasting. It is clear from internal or shared loss databases that operational risk losses show at least an 80–20 Pareto distribution. In reality, 5% of major losses explain 95% of the total loss amount. So the major risks or scenarios drive operational risk costs.

The loss distribution approach, commonly in use in Europe and North America for more than 10 years, is based on the idea that potential large losses can be extrapolated from recurring losses. This idea is simply wrong. There is no logic in extrapolating repeated individual credit card frauds into a large merchant or payment processor compromise, such as the recent Target data breach. There is no logic in extrapolating individual lawsuits into a major class action. The underlying mechanisms and, in most cases, the exposures are not the same.

Using the loss distribution approach (LDA) is in reality extrapolating waves to predict a tsunami. But waves are produced by wind, and tsunamis by seismic activity – a tsunami is not an unexpectedly big wave.

Although I would agree with some of my colleagues that the standardised measurement approach (SMA) for operational risk has many flaws, this change could drive the adoption of more rational approaches for modelling operational risks outside of the capital quantification framework.

As operational risk was driven by regulatory requirements, usually with a short-term perspective, the typical and practical response by the banks was to create an application for each regulatory requirement – capital calculation, stress tests, risk management, and so on – for an organisation or team to act upon. Risk control self-assessment registers were designed to reflect business processes and to be able to develop controls. Models were designed by quants and structured in a meaningless way for business, and units of measurement were created in such a way that statistical laws could fit the data. This is probably the most extreme data-driven approach I have seen as a modeller in decades: the imposition of an artificial structure to data in order to fit statistical laws.

Using available knowledge to inform risk analysis

With the likely adoption of the SMA, the regulatory pressures for quantification may subside. It is probably a good time to think differently and try to build a single application that will answer all requirements and, therefore, maintain stability as regulations evolve. This single approach could then be used for capital calculation, stress testing, risk management, allocation and challenge. This is an especially important objective today, as many efforts made to implement the advanced measurement approach in the past 10 years are about to be discarded, and the general message delivered by the Basel Committee on Banking Supervision is that 'operational risk cannot be modelled'.

Before addressing this issue, let us identify which data or knowledge is available to model operational risk.

On one hand we have all the data/knowledge related to operational risk losses or events: internal losses, external losses that could be obtained from consortia and scenarios. For now, let us define scenarios as the analysis of particular situations that could generate large operational losses, and the unfolding of these situations.

On the other hand, we have information on the firm: its business, measured by various indicators, business variables that express the exposures of the firm, and macroeconomic variables and correlations that potentially express the context and how operational risks might be sensitive to this context.

This is the overall picture that needs to be considered to determine how to model operational risk. Two ways of organising this data and knowledge can be considered.

Those following the data-driven point of view try to create an operational risk model as a statistical law, represented by some parameters and inferred from data. All the sources are considered as contributors to the constitution of a loss database. In addition to observed losses, other sources are used to complement the loss database when no event has been observed, in particular potentially extreme events. For instance, these additional data points are generated using scaling or expert scenario assessment. The paradox is that most of the mathematical effort is spent in distribution fitting, while the distribution itself is strongly driven by potentially extreme events assessed qualitatively. One can now start to see the problem created with the LDA – it is almost as if the industry knew the qualitative assessment of the extreme events was critical to the quantification, but decided it was imperative to have a complex statistical model focused on the rest of the information to model the risk.

On the other hand, the scenario-driven point of view is precisely focused on the potential large future losses. Building scenarios means analysing the loss-generating mechanism, which is a forward-looking approach. In the near future, banks will need to consider possible attacks on blockchain as a major operational risk. How will this be addressed? By using statistical data? By extrapolating existing cyber attacks on centralised architectures? We need to understand the possible attacks, how they can unfold and how they can be stopped. In this approach, all information and knowledge is used to inform the loss-generation mechanism.

There is also a key difference in the way the two approaches can be challenged. The data-driven approach can only be challenged by backtesting. The scenario-driven approach can certainly be backtested, but can also be challenged in the details of the mechanism, and scenarios can also be challenged by other experts, by external events, and so on.

Structured scenarios assessment

If we abandon the second misconception of extrapolating losses, we can focus on scenarios, each of which is defined by a particular exposure. Abandoning the first misconception as well – that operational risk is not exposure-based – we can arrive at something we call 'structured scenario assessment'.

This approach can be observed in a rogue-trading scenario, which is a good example of a loss-generation mechanism being described and later turned into a structured scenario. A trader builds and conceals a large directional and unprotected position – naked trading without adequate hedging positions – with the aim of creating large profits once the market moves in favour of the position. The position is detected a few weeks later during a control with a counterparty. However, unwinding the position generates a large loss as the market has moved against the position.

As discussed at the beginning of this article, the exposure to this risk is the number of traders working at the firm. Any of these traders can 'go rogue', thereby exposing the firm to such a loss. The impact will of course depend on the magnitude of the limit breaches and of the duration of the fraud.

The scenario can be broken down into three dimensions:

- Exposure – the traders
- Occurrence – going rogue
- Impact – the market loss when the position is finally discovered and unwound.

Business indicators can be used to assess the number of traders in a position to perpetrate fraud, and internal and external data can be used to assess the probability of a trader going rogue. The size of the position that can be built and the time to detection can be assessed based on existing controls, both internal and external – relations with counterparties or clearing houses, for instance. Finally, the loss will be dependent on the market movements when the position is unwound, which can be assessed using market data.

Such a structure can also be used for all of the following purposes:

- It can be used to generate a distribution of potential losses according to the loss mechanism. Monte Carlo simulation of all the drivers involved in the model is used, i.e. each of the variables driving exposure, occurrence or impact. Once the distribution is built, the percentiles can be observed and used for capital calculation. This can be very different from extrapolating loss data or asking experts to directly assess the 1/20, 1/50 and 1/100 events.
- Stress testing can be performed on drivers, rather than relying on external correlations. If we consider an adverse scenario, we can explicitly stress one or more of the scenario variables. For example, if a rogue-trading event occurs in a highly volatile market, the losses might be higher, but some controls such as margin call monitoring could also be less efficient.
- Risk management can be directly represented in the loss-generation mechanism. Again, assuming that a stronger and more systematic control of positions with counterparties would detect a concealed position sooner, one might consider the benefit of this control on the cost of the risk.
- Capital allocation is straightforward. Most of the time this is performed through the allocation of the exposure units. But it can be also reflected in stronger or weaker controls, depending on the line of business or legal entities.
- Finally, the scenario challenge is certainly more robust. When using a purely expert approach, the challenge meetings are usually boring: too high, too low, etc. In that case it is very easy to identify weaknesses in the scenario: incomplete exposure, missing key driver, and so on.

Conclusion

There are sound methods for addressing operational risk modelling, as long as it is approached with a simple guideline: the need to understand and analyse the loss-generating mechanism for possible future material risks. In addressing the problem from this angle, banks and other financial institutions should be able to collect and organise valuable knowledge about their major operational risk exposures.

It is nevertheless necessary to establish an appropriate organisation in order that this endeavour be successful. In particular, it is advised that the role of the second line is strengthened – it has an important role to play in analysing scenarios that can exceed the expertise of the first line. But this would be the subject of another article.

Contact

Patrick Naim • President
T +33 6 08 34 10 01
E patrick.naim@elseware.fr

www.elseware.fr