Dr. Bahram Mirzai, *CEFA is Managing Partner at EVMTech, a company specialising in operational risk. He has more than seven years experience in risk management. In his last position he worked as senior vice president and chief actuary for Swiss Re's Global Banking Practice. He has led numerous consulting assignments with leading banks on operational risk management and has been frequently invited by regulators to speak on operational risk matters.*

Dr. Mikhail Makarov *is Managing Partner at EVMTech, a company specialising in operational risk. He has more than five years of experience in risk management and has previously worked as an actuary at Swiss Re and as a lecturer at Ohio State University.*

Operational risk – COSO re-examined

Peyman Mestchian, SAS EMEA;
Mikhail Makarov, EVMTech;
Bahram Mirzai, EVMTech

Operational risk, albeit not a new risk discipline, has gained fresh impetus in the light of Basel II. In order to promote and advance operational risk as a recognised and respected risk management discipline, several criteria need to be met:

1. There needs to be a framework for operational risk management together with a common language across the industry;
2. A set of appropriate risk management techniques and tools should be developed;
3. Firms need a thorough understanding of their business processes.

The first two requirements are generic in nature, and therefore one can expect the methods developed for enterprise risk management to be applicable here as well. A number of institutions have considered applying the Committee for Sponsoring Organisations of the Treadway Commission (COSO) framework for operational risk management.

The COSO approach is described in the *Enterprise Risk Management—Integrated Framework* papers authored by COSO in 2004 [1, 2]. The Framework paper outlines an integrated approach to enterprise risk management. The Technical Application paper provides an overview of the methods and techniques used in enterprise risk management.

Application of the COSO framework to operational risk has been recently criticised by Ali Samad-Khan [3]. We believe that although the effectiveness of the COSO framework for operational risk remains to be seen in practice, the arguments put forward by Samad-Khan are at best misinformed and at worst irresponsible.

Misinformed, because the primary focus on unexpected loss in his article defies the very principles of the Basel II Accord – namely the promotion of risk governance, risk management (identification, assessment, monitoring and control/mitigation), and risk disclosure [4].

Operational risk is defined by the Basel Committee as "the risk of loss resulting from inadequate or failed business processes, people and systems or from external events". Unexpected loss relates primarily to capital adequacy under Pillar 1. However, there is more to risk management than capital adequacy. Consequently, Pillar 2 stresses the importance of a sound system of internal control and governance structure. It is through a COSO-type risk assessment approach that different risk management needs can be aligned and integrated within one framework.

A recent paper presented to the Institute of Actuaries: "Quantifying Operational Risk in General Insurance Companies" [5] deviates from applying the traditional purely statistical approaches and concludes:

"Whilst not purely strictly actuarial in some past senses of the word, this [operational risk management] means beginning by identifying, assessing and understanding operational risk, and being able to view various forms of control as important, as well as understanding their impact – all before using statistical measurement techniques. This requires insight into, and understanding of process management, organisational design including defining roles and responsibilities, occupational psychology and general management. The actuarial analytic training is good grounding for such work, but by no means a passport to success."

Samad-Khan's comments are irresponsible because a "reverse engineering" of some high-profile operational risk failures in the banking history e.g. AIB, Barings or Sumitomo, shows that such events could have been avoided or discovered in an early stage if a sound and integrated risk management framework had been *practiced*.

In the case of Barings, evidence has shown that COSO-based audits did actually identify and assess the risks correctly (e.g. lack of proper segregation of duties), but senior management chose to ignore many of the assessment results. In fact, it is the study of such major failures that has resulted in COSO-based regulations such as Sarbanes-Oxley and risk-based auditing, which is at the heart of most modern financial auditing standards. History has shown that it is dangerous to ignore this evidence both from methodological and legal points of view.

The COSO-based risk assessment has been widely used in the risk management industry for many years in the financial and non-financial industries. An example of this is the approach advocated by the UK's Financial Services Authority, who says in Consultation Paper 142:

"A key issue is operational risk measurement. Due to both data limitations and lack of high-powered analysis tools, a number of operational risks cannot be measured accurately in a quantitative manner at the present time. So we use the term risk assessment in place of measurement, to encompass more qualitative processes, including for example the scoring of risks as 'high', 'medium' and 'low'. However, we would still encourage firms to collect data on their operational risks and to use measurement tools where this is possible and appropriate. We believe that using a combination of both quantitative and qualitative tools is the best approach to understanding the significance of a firm's operational risks."

The criticism provided by Samad-Khan is based on the following main points:

1. The definition of the risk used by COSO is flawed;
2. A likelihood-impact risk assessment is flawed;
3. Methods prescribed by COSO are highly subjective, and only risk assessment based on historic losses is valid;
4. Risk assessment using COSO approach is too complex and resource intense.

In the following section we would like to comment on each of these points in some detail.

Definition of risk

Samad-Khan's argument around the flawed definition of risk is based on the equation:

Risk = Likelihood x Impact.

There is no reference in COSO publications [1, 2] that this formula is used as a measure of risk. On the contrary, the COSO framework suggests use of Value at Risk or Capital at Risk concepts as measures of risk.

Samad-Khan's discussion of expected and unexpected loss may also lead to the wrong impression that only unexpected loss should be of importance for management of operational risk. According to such a view, a $100 million loss in credit card frauds which occurs every year and thus has an expected loss contribution of $100 million and zero unexpected loss contribution should not be considered for risk assessment.

In fact what is important is the cost of risk expressed as

Cost of Risk = Expected Loss + Cost of Capital.

In other words, the cost of risk (CoR) is the sum of the expected loss and the cost of capital required to cover the unexpected loss.

To illustrate how this formula is applied let us consider an example. Suppose that a bank has on average $300 million of operational risk losses per annum and holds $1.5 billion of capital to cover the unexpected loss. Assuming that the cost of the capital for the bank is 5%, the CoR becomes:

Cost of Risk = 300 + 5% x 1500= $375 million.

Evaluation of the CoR is crucial to perform cost-benefit analysis within an integrated operational risk management framework, e.g., an organisation's willingness to take a risk will depend on whether or not the CoR justifies the anticipated returns. As the example shows, expected loss can play a dominant role in the analysis of the CoR.

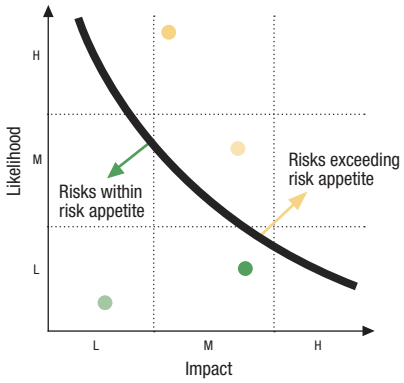
For most risks, the contribution to the unexpected loss to CoR will be small and CoR will mainly be driven by the expected loss. It is only for rare and severe impact risks that the CoR is driven by the cost of capital.

Consequently most of the reduction in CoR will come from the reduction in the expected loss. In this respect a COSO type framework, which not only focuses on management of rare risks but also on common risks, will prove useful.

Likelihood-impact based risk assessment

One of the approaches considered in the COSO framework is the likelihood-impact assessment. The likelihood-impact assessment was originally introduced in MIL-STD-882A – a military system safety standard introduced by the US Department of Defense. This landmark document has been widely and successfully used by risk and safety practitioners since its introduction in 1977.

Figure 1: An example of a risk assessment using the likelihood-impact method.



This approach maps different risks into a matrix similar to the one shown in Figure 1.

According to this approach, for each risk the frequency of occurrence (likelihood) and the worst credible outcome (impact) are assessed and captured into a likelihood-impact matrix.

The likelihood-impact matrix is then compared with the risk appetite map. The risk appetite map outlines the maximum level of adverse risk outcome that an organisation is willing to accept. As a result of the comparison, any significant risk exceeding the risk appetite will call for management action. The matrix not only helps risk assessment but also allows portraying of risks.

Risk assessment is often not performed in terms of distributions but rather the results of a risk assessment are translated into severity and frequency distributions. A well-known example of risk assessment is the credit rating of a company where the outcome of the assessment, e.g. company rating, is translated into frequency and severity distributions.

Samad-Khan's criticism of the likelihood-impact approach is based on a misunderstanding. When likelihood-impact assessment is used to check whether or not a risk exceeds the risk appetite levels, it is sufficient to estimate only frequency and worst outcomes of the risks. However, when a comprehensive risk assessment is required, one needs to estimate likelihood and impact for several outcomes of the risk.

For example, in a manner similar to credit risk assessment, it is possible to estimate frequency of losses (PD in credit terminology), expected impact (LGD in credit terminology) and worst credible impact (EAD in credit terminology). Cleary the results of such risk assessment can be translated into frequency and severity distributions, Fig 2.

Subjective versus statistical risk assessment

It is interesting to observe the degree of antagonism between "business experts" and "statisticians". Business experts insist on use of subjective risk assessment and compare statistical analysis to driving a car by looking in the rear view mirror only. Statisticians on the other hand argue that subjective assessment is best comparable to predicting the future by looking into a crystal ball.

Modern risk management frameworks such as Basel II, COSO or MIL-STD-882 require integrated approaches combining both subjective and data driven risk assessment. The weight assigned to each approach is dependent on the degree of confidence given to each set of information.

The necessity for using both approaches becomes especially apparent when assessing rare risks with extreme impact such as the World Trade Cetner or Tsunami events. Of course one may choose not to take into account the terrorism alert levels issued by the US government, since they incorporate some subjective judgment.

The practice of risk management shows that successful organisations have adopted a balanced and complementary approach using both subjective and data-driven risk assessment methods. Figure 3 describes some examples of quantitative and qualitative techniques applicable to operational risk management.

Complexity of assessment process

The argument as to the complexity and resource intensiveness of a COSO-type risk assessment is a misleading one. There are numerous examples that such approaches have been applied with consider-

Figure 2: Cumulative distributions of severity and aggregate risk.

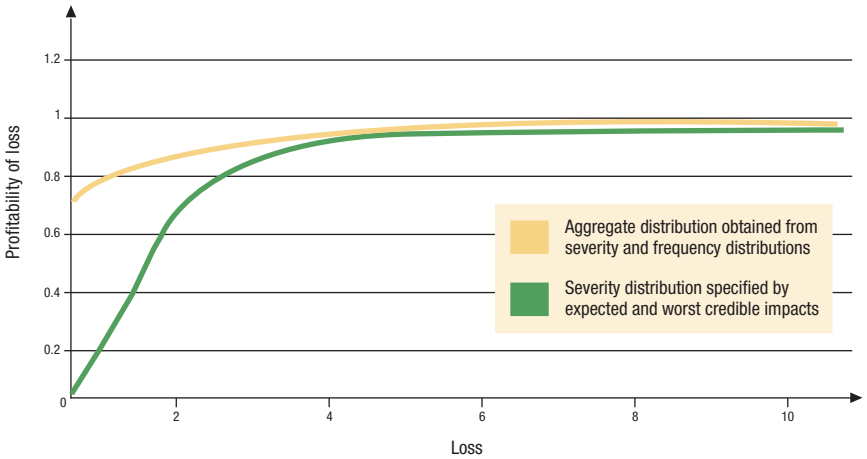
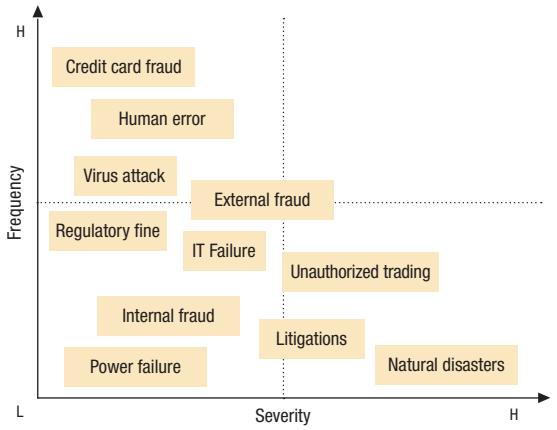


Figure 3: Examples of qualitative and quantitative techniques.



High frequency + low severity
Plenty of loss data and potential for use of statistical techniques and process systems (six sigma total quality management, automated pattern recognition for fraud detection, etc.

Medium frequency + medium severity
Risk and control self-assessment, scenarios analysis and audit mechanisms – combination of qualitative and quantitative techniques. Potential for causal modeling.

Low frequency + high severity
Actuarial techniques such as LDA, EVT supported by qualitative techniques such as self-assessment and scenario analysis, use of external data.

able success. The pioneering work embodied in MIL-STD-882 has been incorporated into system safety standards used in, for example, the chemical processing industry (EPA's 40CFR68) and the medical device industry (the Food and Drug Administration's requirements for Pre-Market Notification). The semi-conductor manufacturing and nuclear power industries use many system safety analytical techniques during the design of production processes, equipment and facilities, principally because the cost of "mistakes" is enormous in terms of production capability, product quality and, ultimately, human life.

Obviously operational risk management focus is not simply a more accurate measurement of risk but also a reduction of operational losses and the overall cost of operational risk. For most financial institutions a reduction of expected loss in the order of 10 percent would be sufficient to justify the risk assessment process and to cover the cost of resources. We believe that the development of operational risk framework, tools and management techniques that would allow firms to reduce operational risk losses will remain a key priority beyond the implementation deadlines of Basel II.

Conclusion

We strongly believe that the primary goal of operational risk management should be business success and value creation – more so than the fear of failing compliance tests or even ensuring capital adequacy – vital though these two secondary motivations should be.

The science and practice of operational risk management is evolving rapidly. To be successful, practitioners should be taking a multi-disciplinary approach bringing together the best of the disciplines of statistics, process management, finance, organisational design, total quality management and business strategy. Operational risk practitioners should be wary of specialists who are dogmatic in their approach. Ultimately, if the only tool in your tool-box is a hammer, every problem will start to look like a nail. To exclude any specific approaches or framework at the current stage of evolution of the subject is bound to result in a flawed and narrow-minded solution. Operational risk management requires practitioners with open minds, the ability to learn from others and the flexibility to explore other methodologies.

References

[1] *Enterprise Risk Management – Integrated Framework:* Executive Summary and Framework, by the Committee of Sponsoring Organisations of the Treadway Commission, 2004.

[2] *Enterprise Risk Management – Integrated Framework: Technical Applications,* by the Committee of Sponsoring Organisations of the Treadway Commission, 2004.

[3] *Why COSO is flawed,* by Ali Samad-Khan, OperationalRisk, January 2005.

[4] *Sound Practices for the Management and Supervision of Operational Risk,* Basel Committee on Banking Supervision, February 2003.

[5] *Quantifying Operational Risk in General Insurance Companies,* developed by a Giro Working Party presented to the Institute of Actuaries, March 2004.