



## Practical operational risk management: part one

Nov 13 2008 [Philippa Girling](#)

This article is the first in a series on practical operational risk management. The series will look into the practical aspects of building and maintaining an effective operational risk management program.



Philippa Girling

### Building an effective operational risk framework

Operational risk management has arisen as a discipline as a result of influences from three main sources: regulators, senior managers and third parties. The first comes from recently amended regulatory requirements. The strongest incentives for operational risk management are Basel II compliance for global banks and Solvency II compliance for insurance firms. Basel II was developed in the European Union as a new, more sophisticated approach to risk. Basel II has three pillars. Pillar one concerns the risk management practices and capital requirements for market, credit and operational risk. Pillar two concerns the role of the regulator in enforcing these standards and addresses the risk management and capital required for "material other risks" such as reputational risk and strategic risk. Pillar three concerns the public disclosure of risk measures and capital calculations by the firm.

The definition of operational risk according to Basel II is: "Operational risk is defined as the risk of loss resulting from inadequate or failed processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk."

Solvency II addresses risk management for the insurance industry in similar ways.

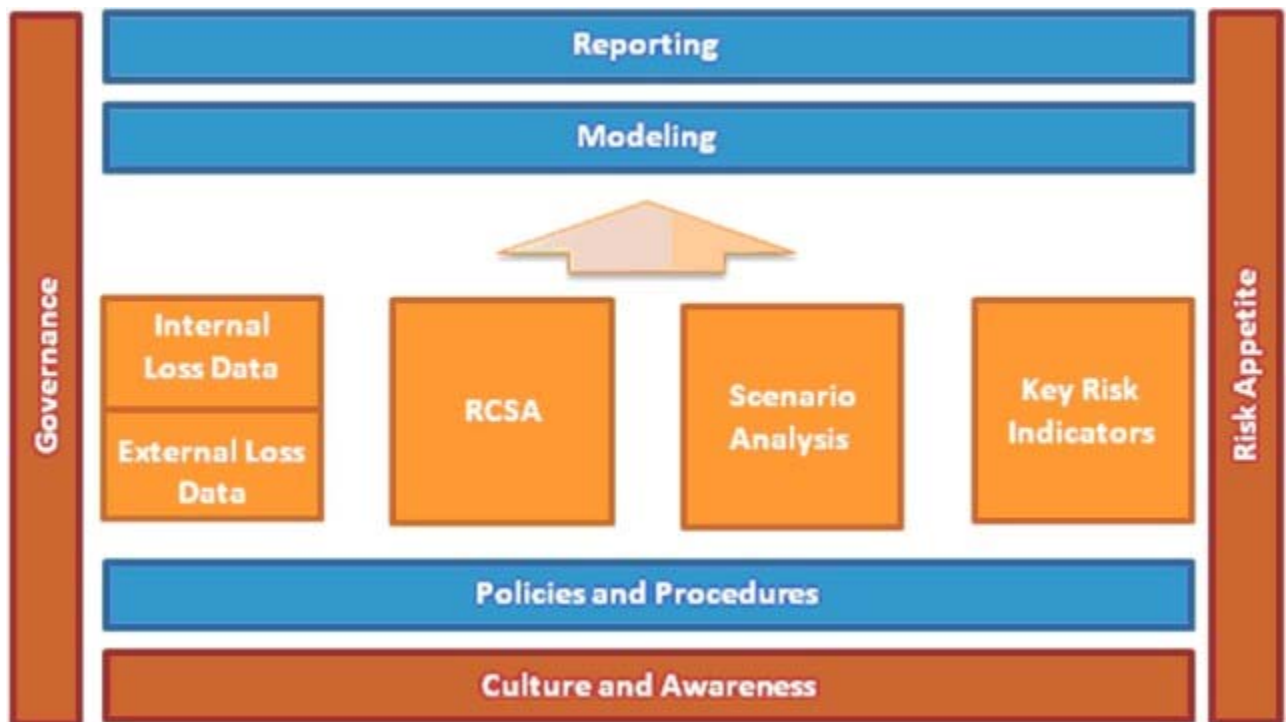
The second influence for operational risk comes from within the firms themselves. Large operational risk events have the potential to cause severe capital and reputational damage to a firm. Without an effective

operational risk management program in place, senior managers are unable to determine whether their exposure to operational risk is a concern or not. A new transparency of risk severity is needed and tools are being sought to provide the executive team with the operational risk information that they want. The third influence comes from external third parties which have started to ask about the operational robustness of a firm. Ratings agencies, investors and research analysts are becoming educated on the potential catastrophic impact of operational risk events and so are asking tougher questions. They want to know if an effective operational risk framework is in place and if enough capital is being held to protect a firm from a rare, catastrophic event.

In response to these three influences, operational risk programs have sprung up globally across many industries. There has been a particular enthusiasm in the financial services industry due to the Basel II requirements that many firms have needed to meet. To be Basel II-compliant a firm must adopt one of three possible approaches: basic, standardized or advanced management approach. The options for these depend on the local regulators interpretation of Basel II. Generally, banks that are more sophisticated must adopt approaches that are more sophisticated. Regardless of the approach taken, pillar two requires best practice. In addition, the other two influences — senior managers' need for risk transparency and external parties deepening interest in operational risk excellence — push operational risk programs into best practice rather than minimum standards.

What then should a robust operational risk framework look like and how can a firm ensure that operational risk is being effectively managed? Basel II requires that operational risk is identified, assessed, controlled and offset. It recommends that firms adopt the sound practices for the management and supervision of operational risk. As a result, the elements in an operational risk program often include loss data collection, risk and control self-assessments, scenario analysis and key risk indicators. There are also modeling requirements for capital calculations and reporting requirements to meet pillar three disclosure and to demonstrate active consideration of operational risk across the firm. These elements need to be placed in a framework that has an appropriate governance structure, policies and procedures, culture change and education activities. These must all respond to, and inform, risk appetite.

The diagram below illustrates a possible framework that captures these elements:



This series will consider each of these elements and will dig deeply into each element to discover what the potential pitfalls are, where value can be extracted, how operational risk is being identified, assessed, controlled and offset, and most importantly, it will ask the question "so what?" You have collected loss data

— so what? Your risk and control self-assessment program is up and running — so what? You have identified key scenarios — so what? You have 150 key risk indicators reporting every month — so what?

These articles will consider how to ensure that the operational risk management program is not a data collection program, but rather a sophisticated operational risk analysis program that provides transparency of risk and that informs the risk appetite of the firm. They will also consider how each element can move forward the culture change that is needed to truly embed operational risk management in a firm. The practicalities of designing and implementing elements that will fit the firm and be accepted by its employees, from senior managers to junior staff, will be considered. How to avoid that "so what?" question will also be looked at, by delivering reporting that matters.

### **Governance and culture and awareness**

All of the elements are important; however, the order in which they are implemented will depend on the current needs of the firm and on the three influences: regulatory, senior managers and external parties. There are two elements that should always be addressed first: "governance" and "culture and awareness".

Without appropriate governance in place, the owners of the operational risk management program will flounder on the rocks. The operational risk management team needs to have a reporting structure which will empower it when necessary and that will review and approve the strategic framework that is being rolled out. There are many different governance approaches that are available and these will be considered in the next issue of this series. The governance approach needs to reflect the culture, complexity and strategy of the firm and must be practical and effective. In the meantime, until governance has been established, the rest of the framework will be difficult or even impossible to implement. The governance structure holds the framework together, as illustrated in the above diagram.

The bedrock of the operational risk framework will be the culture and awareness element. All other elements will rely upon a base understanding and buy-in to operational risk management. This requires serious practical activities by the operational risk management team. This is an area where marketing and organizational change skills are needed within the operational risk team. The more effort that is expended on this element, the more smoothly the other elements will be implemented across the firm.

Above the culture and awareness element lies policy and procedure. Policies and procedures for operational risk will need to be developed and amended as the framework evolves. These have an important role in regulatory compliance and need to be considered carefully and should be maintained rigorously. Above the policy and procedures element sit the four main blocks of work which the firm will undertake to meet its goal to identify, assess, control and offset operational risk: loss data (internal and external), risk and control self-assessment, scenario analysis and key risk indicators. These four elements will inform the modeling and reporting elements.

Finally the risk appetite of the firm will be derived, considered and addressed throughout the framework. Once articulated, risk appetite can be used to mould the operational risk framework and prioritize activities within it. Risk appetite is listed last here, as it is the most difficult to address and requires some experience before it is well understood and expressed, and the framework will be under development before risk appetite is clarified. The operational risk team is required to plan, document and market carefully, and the governance structure should support, each of these framework elements. The design and implementation of an operational risk structure that works for a firm requires a careful balancing of the three influences and the culture of the firm. The practical steps and considerations for the successful implementation of each of these elements will be considered throughout the series.

*Philippa Girling is an Of Counsel Attorney at Garrity, Graham, Murphy, Garofalo and Flinn in New York. She was previously global co-head of operational risk management at Nomura.*

*This article first appeared on Complanet on [www.complanet.com](http://www.complanet.com) on November 13 2008. For a free trial of Complanet's services, please contact client support on [client.support@complanet.com](mailto:client.support@complanet.com) or +44 (0) 870 042 6400.*