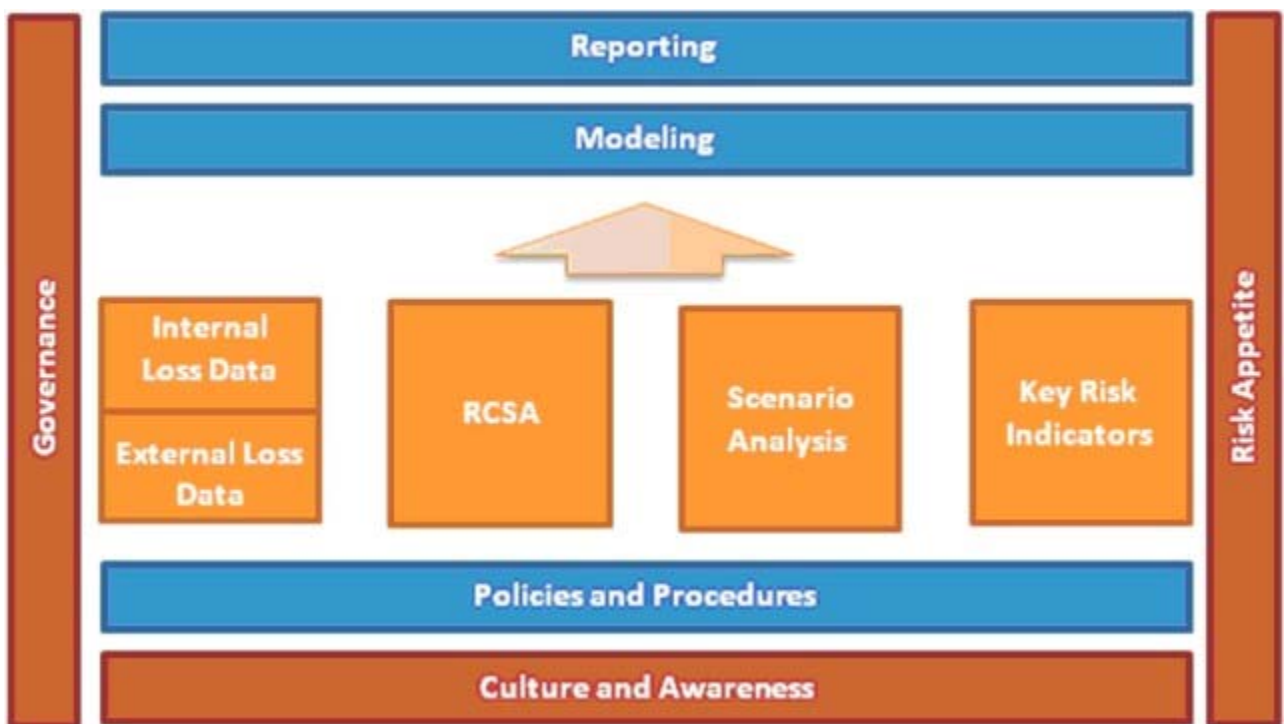




Practical operational risk management: part two — governance and integration

Dec 30 2008 [Philippa Girling](#)

This article is the second in a series on practical operational risk management. The series looks into the practical aspects of building, maintaining and driving forward an effective operational risk management program. The [first](#) article briefly looked at all of the elements that are needed for an effective operational risk framework as below:



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 drivers of operational risk management: regulatory, senior management 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 founder on the rocks. The operational risk management team needs to have a reporting structure which will empower it when necessary and supportive management that will review and approve the strategic framework that is being rolled out. The governance approach needs to reflect the culture, complexity and

strategy of the firm and must be practical and effective. Until governance has been established, the rest of the framework will be difficult or even impossible to implement.

There are two main considerations that will drive the governance structure:

1. Who should own the operational risk function?
2. What should the operational risk function own?

When answering these questions, it is necessary to consider the two perspectives of operational risk: operational risk *management* and operational risk *measurement*. Operational risk management is focused on identifying, assessing, controlling and mitigating operational risk. In contrast, operational risk measurement is focused on the capital calculation. There are measurement aspects to operational risk management; however, these tend to be qualitative assessments, i.e., high, medium or low risk, whereas the capital calculation is focused on quantitative assessments, i.e., dollars at risk. It is important to maintain a healthy balance between the two perspectives of the framework. The right balance will depend on the influences within a firm.

Who should own the operational risk function?

Many operational risk functions started life in the operations department. Sometimes this was due to a misunderstanding of the definition, as "operations" risk sounded temptingly like "operational" risk. The operations department owns many operational risks, although obviously operational risk exists across the whole firm. Often a dedicated operational risk function remains in the operations department, but the firm-wide operational risk function will need to be placed in a central location that meets three criteria: independence, importance and relevance.

When assessing whether the current location of the firm-wide operational risk department is appropriate, it should be considered in the light of those three criteria. Does the current location ensure the independence of the operational risk function? Does it provide appropriate importance for the function? Is the operational risk function considered relevant within the organization? If any of these questions are answered "no" then it may be necessary to reconsider the current governance structure. There are various options for the upward governance of operational risk. Who could own operational risk and what are the advantages and disadvantages of each option?

The chief risk officer, or the risk department, owns operational risk



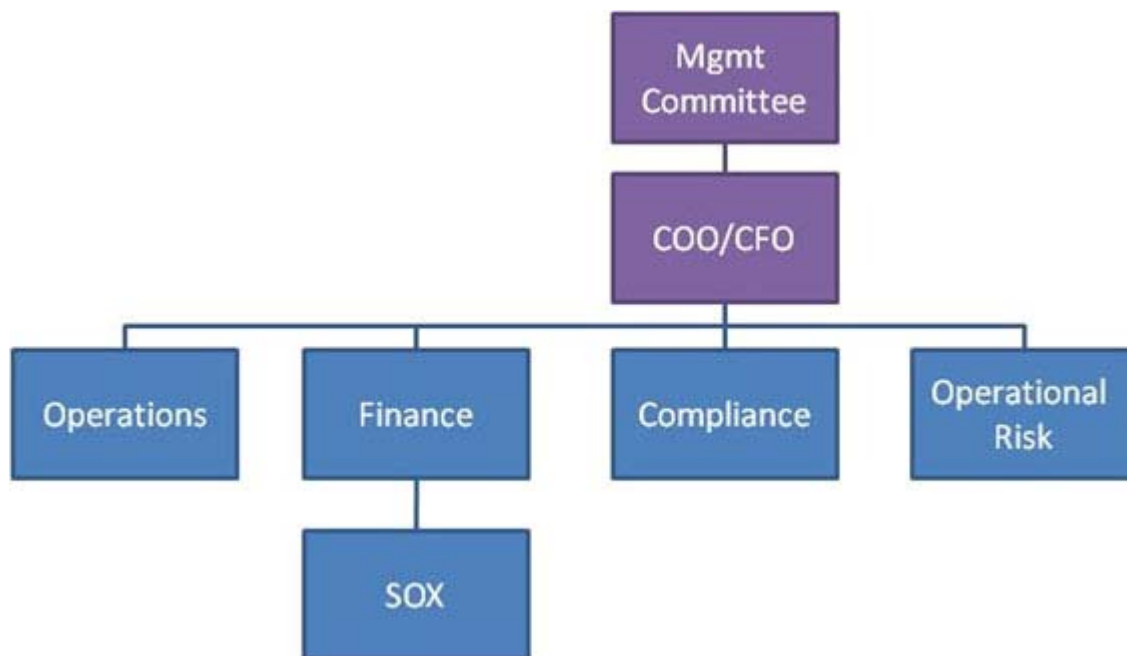
There are several advantages to such a structure. First, the independence of the operational risk structure is clear — the chief risk officer sits outside the business lines and support functions and so provides the operational risk department with the independence it needs. In addition, the risk function is considered important in most, if not all, firms and the operational risk department can inherit that importance by being part of the risk governance structure.

For an operational risk manager, there is a definite advantage in sitting at the same table as the market and credit risk managers. There is an opportunity to identify synergies between the risk categories and the learning between the risk functions can provide a more holistic and effective risk management viewpoint for the firm. As market risk identifies major factors that affect its value at risk calculations, the operational risk department can, therefore, gather important information on changes in the business environment that may affect operational risk and control ratings. An external operational risk event may also be of real interest to the credit risk party, if that event occurred in one of the firm's counterparties.

This close working relationship with the other risk functions provides the firm with the opportunity to develop an enterprise risk management approach to risk, which looks not just at one element of risk at a time, but all elements together. One disadvantage of such a structure, however, can sometimes be a practical one. If there is a single risk committee meeting each month, it is not uncommon for market and credit risk to dominate that meeting, which leaves operational risk with a five-minute slot in which to summarize its key findings and recommendations for the month. A separate dedicated operational risk committee can overcome this problem.

An additional disadvantage can be that the operational risk function is seen as separate from the other support functions of the firm, and it may lead to more challenges in developing effective partnerships with important owners of operational risk across the firm, such as the Sarbanes-Oxley team, the legal and compliance department, and the operations, IT and finance functions.

The chief operations officer, or the chief financial officer, owns operational risk

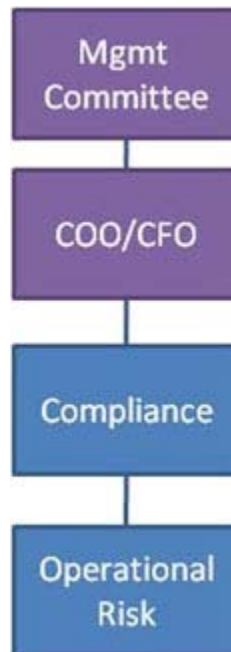


This second governance structure option also has its own advantages and disadvantages. It is not unusual for a firm-wide operational risk department to report into a COO, a chief administrative officer, or a CFO role. The advantage of such a structure is that the senior manager who has ownership of all those areas can encourage (or even mandate) the relationships between the operational risk department and those departments that already own and manage operational risk. For example, if the CFO owns both the SOX team and the operational risk team, then they are more likely to insist that there is an effective working relationship between them, therefore cutting through some of the politics that are often involved.

In such a structure there is an increased opportunity for convergence and governance, risk and control initiatives. Such initiatives are designed to ensure that all data is collected, assessed and stored only once, and that each consumer can go to a central source for consistent data. GRC initiatives also provide opportunities for increased efficiency, reduced redundancy and richer reporting. A disadvantage of such a structure is that it may be challenging for the operational risk department to demonstrate independence.

Departments within the same reporting structure may own much of the operational risk, which might suggest that the operational risk department is limited in its ability to remain impartial and objective. In practice, an operational risk department will always have independence issues at some level. After all, operational risk exists within the operational risk department itself. A strong set of policies and procedures can overcome this.

The compliance department owns the operational risk



Another option for governance is for the operational risk function to report into the compliance department. The advantage of such an approach is that the operational risk function can quickly and easily inherit a reporting structure, along with meeting schedules and reporting cycles. It can also work in partnership with compliance to leverage its data and assessment activities. The disadvantages are that the operational risk function can appear to be too removed from the business of the firm and may also be perceived as a policing function, rather than as a trusted adviser or facilitator of risk management. There is also less opportunity for a strong working relationship with market and credit risk. It is worth noting that the operational risk function cannot report into the audit function as it must remain independent and is subject to regular internal audits.

What should the operational risk function own?

In addition to deciding what the upward governance structure should be for operational risk to ensure that it is independent, important and relevant, each firm must consider what would be the most appropriate downward governance structure. In other words, what should report into operational risk? There are many potential candidates:

- **OR coordinators**

To manage the many challenges of an operational risk framework, it may be prudent to identify individuals in each business line and support area that are responsible for embedding the operational risk function there. OR coordinators are often not full-time operational risk managers, but have other responsibilities for the majority of their time. OR coordinators could have a direct, or a dotted line, into the operational risk department.

- **Business continuity planning**

BCP functions own the planning for operational risk events that may disrupt the business. These are not just IT disaster recovery activities, but also include response plans for pandemic flu, terrorist attacks and weather catastrophes. It is becoming more and more common for BCP functions to report into the head of operational risk.

- **Information security**

Information security functions sometimes suffer from a lack of independence, especially if they report into the head of IT. Placing information security in a reporting line to operational risk can, therefore, provide a more appropriate governance structure. Information security is an operational risk area and the activities, controls and policies of the information security function can be developed in close partnership with, or under the guidance of, the operational risk function. It is becoming more and more common for information security functions to report into the head of operational risk.

- **Sarbanes-Oxley**

SOX addresses the risk of a financial misstatement and, as such, is a subset of operational risk. The level of detail that is required for SOX purposes might be more than is needed for the rest of the operational risk program, but the SOX controls, risks, assessments and action items can be developed in close partnership with, or under the guidance of, the operational risk function. The SOX risk and control scores should be incorporated into any operational risk assessment work that is undertaken. It is becoming more and more common for SOX functions to report into the head of operational risk.

- **Audit point tracking**

Audit assigns issues and action items and these often overlap with, or are relevant to, operational risk and/or SOX action items. To provide efficient reporting and tracking of open issues and action items across a firm, an operational risk function might take on responsibility for tracking progress on all action items and may provide consolidated action tracking or issue reporting to senior managers.

- **New business approval or new product approval**

Most firms have developed policies, procedures and processes to manage the launching of new products or businesses. The new product approval process is designed to ensure that all aspects of the new venture have been considered — from risk to operations, from finance to IT requirements and so on. Operational risk might have one of several roles, for example, it could own the whole process, it could be a required signatory for new ventures or it might require that all departments consider operational risk when giving their sign-offs.

Once a robust and appropriate governance structure has been implemented for operational risk, the next framework element that must be addressed is culture and awareness. The goal of a culture and awareness program is to educate and engage the firm in effective operational risk management and embed operational risk management at all levels within the organization. The challenges and practicalities of culture and awareness will be considered in the next installment of this 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 on December 30 2008. For a free trial of Complanet's services, please contact client support on client.support@complanet.com or +44 (0) 870 042 6400.