CHAPTER 8

The Management of Operational Risk

8.1 INTRODUCTION

The management of operational risk is not a new idea, neither is it an activity that firms have not indulged in. On the contrary, firms have always striven to manage the risk of fire through insurance and fire safety measures. Furthermore, they have always had specialists who managed other kinds of operational risk, such as the lawyers and other legal specialists who are involved in managing legal risk and the structural engineers who look after buildings and structures. This is typically done both proactively (for example, by providing advice to management prior to signing a contract and by maintaining buildings) and reactively (by providing legal representation in a court of law, representing the firm in out-of-court settlements of disputes, and doing repair work on damaged structures).

8.1.1 Operational risk management in financial institutions

On the issue of whether or not operational risk management has been practiced for some time, Kennett (2003) argues that operational risk has been managed (implicitly) since "year dot". Referring to banks specifically, he argues that "ever since they first opened their doors as banks, operational risk has been at the forefront of their activities". He even claims that most firms have managed operational risk pretty effectively over the years, although there are some obvious examples (most likely, this is reference to Barings Bank, Long-Term Capital Management and the like). Likewise, Buchelt and Unteregger (2004) argue that long before the advent of

Basel II, financial institutions had put in place various control mechanisms and procedures. To combat physical threats, for example, extensive security and safety measures, as well as security rules, have been put in place. They also mention the control roles of the human resources, legal and internal audit departments. A similar view has been put forward by Saxton (2002) who argues that operational risk is not new, but rather a concept that "banks have been struggling with for years with varying degrees of success".

Conversely, the management of market risk and credit risk, particularly by using the relatively recent invention of financial and credit derivatives as hedging devices, was virtually unknown for a long period of time, by a specific name or otherwise. Hence, operational risk management is older than either credit risk management and market risk management. But just like the terms "risk", "financial risk", "market risk", and "credit risk" appeared before the term "operational risk", the terms "risk management", "financial risk management", "market risk management", and "credit risk management" appeared before the term "operational risk management". However, it is not only the name because, unlike credit risk management and market risk management, operational risk management has never been (and it is still not) an integrated process, although it appears that things are moving this way. Rather, operational risk management has been a set of fragmented activities designed to deal with a wide variety of operational risks. We are still a long way away from the target of making operational risk management an integrated process that deals with operational risk as a generic kind of risk. This is not surprising, given that the concept of operational risk was unknown some ten years ago.

8.1.2 The operational risk management lag

What is new about operational risk management (as we know it now) is, according to Hubner et al. (2003), the objective of providing a structure that is comparable to those applicable to credit risk and market risk management. The lag in developing integrated operational risk management relative to credit risk management and market risk management is attributed by Hubner et al. (2003) to the need to bring together information from a range of existing functional units and the resources required for achieving that, as well as the lack of an organizational label (that is, operational risk management) under which these activities could be grouped. The functional units referred to by Hubner et al. include (i) management and financial accounting (information collection, analysis and reporting); (ii) purchasing (contractual terms, outsourcing); (iii) corporate security (the protection of corporate assets from harm); (iv) human resources (background checks on new staff, training in discrimination issues); (v) insurance; (vi) legal and intellectual

property issues (trade marks, copyright, patents); and (vii) audit, both internal and external.

Indeed, Hubner et al. (2003) argue that even though operational risk has been managed inside banks for ever, the development of comprehensive systematic oversight is still at an embryonic stage. Kennett (2003) attributes the lag to several reasons, including the breadth of operational risk, the fact that it is already managed implicitly, the lack of data, the fact that it affects the whole firm, and the fact that a lot of tools and techniques are "more bleeding edges than cutting edges". Moreover, he argues that operational risk management is a "very complex undertaking", more so than either credit or market risk, which are not simple themselves.

Indicative of the lag in the development of operational risk management are the results of three surveys. The British Bankers' Association (1997) conducted a survey of its 300 members, which revealed that many banks had not thought through a definition of operational risk, few had anyone responsible for operational risk and very few attempts had been made to report operational losses in a systematic way. This was contrary to the way banks dealt with credit risk, in which case even relatively small losses were reported. The other survey was commissioned by the BBA together with ISDA and Robert Morris Associates in 1999 (BBA/ISDA/RMA, 1991). This survey, which was conducted on internationally active banks, showed that although much work had been done in the interim, there was still a lot of work to do. Marshall and Heffes (2003) report the results of a survey conducted by the Risk Water Group and SAS involving 400 risk managers at 300 financial institutions. The survey revealed that one in five financial institutions still does not have an operational risk management program although 90 percent of them lose more than $10 million a year due to the poor risk control practices. The survey also showed that a third of them expect to spend less than $1 million a year on the improvement of their risk management practices.

8.1.3 Operational risk management as an integrated process

A growing desire has emerged to organize the components of operational risk into what Hubner et al. (2003) call a "coherent structural framework". They explain the drive to orgainze the operational risk management process to: (i) shareholder value and competition, (ii) senior management and corporate governance issues, and (iii) regulatory issues. The rising importance of shareholders means that they can influence the way in which the firm conducts its affairs, which affects its competitive position. For an operational risk management framework to be effective, therefore, it is desirable to have the endorsement of shareholders. Senior management comes in to determine risk tolerance (or risk appetite) and formulate the corporate

governance statement. For example, should operational risk management be reactive (such as fire fighting, crisis management and clean-up management) or proactive, consisting of data collection and risk assessment, risk control and mitigation and review of approach and enhancement? We have dealt, on more than one occasion, with the role of the regulators. The Basel II Accord is not only concerned with capital adequacy but also with sound risk (particularly operational risk) management.

There is definitely growing tendency to promote the perception of operational risk management as a discipline ranking alongside credit and market risk management and one that is necessary for an integrated risk management framework. This requires clear borders between operational risk, on the one hand, and credit risk and market risk on the other. One of the objectives of establishing the operational risk management function is to help the co-ordination of the application of specialist skills because co-ordination encourages greater communication and transparency.

8.2 WHO IS RESPONSIBLE FOR OPERATIONAL RISK?

A question arises as to who is responsible for operational risk, and this question might be interpreted to mean two different things. The first interpretation is that the question refers to the risk "owners", the risk takers who indulge in activities that lead to operational risk. The second interpretation is that it refers to who is responsible for managing operational risk, whether it is the risk owner or a more centralized corporate body. This is, therefore, a corporate governance issue.

In the broadest sense, risk management should be integrated into the activities of the risk-takers in the firm. But for an independent risk management structure to operate, there has to be an oversight activity that works independently of the risk takers. In the case of market risk and credit risk there is, as a result of many years of experience, a well-established concept of how the activity should function. For operational risk, the issue is somewhat more complicated because the ownership of, or responsibility for, operational risk is not clear. Hubner et al. (2003) put forward the view that the business lines are responsible for operational risk, which means that the responsibility is aligned with profit centers and risk takers. This is intuitively obvious for credit risk and market risk, as they are transaction-focused. The regulatory view embodied in Basel II appears to support the assumption that the business lines are responsible for its day-to-day management. But the problem with this view is that operational risk does not only pertain to profit centers, because it is a firm-wide kind of risk (recall the distinction between operational risk and operations risk).

This characteristic of operational risk creates some problems when we try to set a role for the support functional units (such as human resources

management, IT, security, legal affairs and finance) in operational risk management. In practice, the functional units conduct activities on behalf of the risk owners and also act as advisors, providing not only reactive but also proactive support for the business units. The formalization of the operational risk management process means that there needs to be clarity over the interaction between risk owners and functional support units. The problem here is that functional support units are themselves exposed to operational risk. For example, the human resources department of a firm is a support unit that is exposed to operational risk (such as the legal risk of litigation against the firm by an unhappy employee). Moreover, it is sometimes not clear who the risk owner is. For example, who is responsible for the risk of the theft of information (stored electronically) that results in losses on some foreign exchange positions? Would it be the security department or the IT department (both of which are support units) or would it be the foreign exchange department (which is a business line or profit center)?

The concept of governance models invariably appears in any discussion of operational risk management. While the traditional view is that the responsibility for risk rests with line management, a new governance model is evolving in financial institutions. This model is characterized by having a central operational risk manager, most often reporting to the chief risk officer. The role is one of policy setting, development of tools, co-ordination, analysis and benchmarking, and integration and aggregation of the risk profile. The risk manager would be responsible for setting a common definition for operational risk, developing and facilitating the implementation of common risk management tools (such as risk maps, self-assessment programs and loss event databases), and developing measurement models along the lines described in Chapters 6 and 7. However, the line management remains responsible for the day-to-day risk management activities, since it is the business areas that face the customer, introduce products, manage the majority of people, operate processes and technologies, and deal with other external exposures. Support units develop specific policies and procedures, monitor emerging skills and advise senior management on risk as applicable to their areas.

In addition to the risk manager, line management and support units, risk committees may also be used. The role of a risk committee is to understand the risk profile, ensure that resources are properly allocated and that risk issues are addressed, as well as approving policies, including capital allocation. Haas and Kaiser (2005) suggest the introduction of an "operational risk coach", who would be neutral to all business lines, acting as a confidant, with whom employees could discuss operational loss events and possible solutions without having to fear layoff or negative reputation for themselves or the business line. They suggest that the operational risk coach can be either a member of the committee or reporting directly to it.

In short, therefore, two forms of integrated operational risk management have emerged. Some opt for a mix of the traditional siloed approach and a

touch of firm-wide oversight. While business line managers are closest to the risks to be managed, they lack independence. Under this arrangement, a small corporate risk management department would be in charge of facilitating risk self-assessment. However, firm-wide risk management oversight may be largely absent. Alternatively, there is the centralized risk management approach where there is an established risk management group, which is in charge of (i) setting policies and facilitating the development of operational risk reporting, (ii) independent monitoring, and (iii) establishing key indicators and bottom up empirical capital allocation.

8.3 THE RISK MANAGEMENT FRAMEWORK: STRATEGY

Haunbenstock (2003) identifies the components of the operational risk framework as: (i) strategy, (ii) process, (iii) infrastructure, and (iv) the environment. This section is devoted to the strategy component, whereas the following section deals with the process. The infrastructure and environment are dealt with in a separate section that follows the section on the process.

The strategy involves determination of business objectives, the risk appetite, the organizational approach to risk management, and the approach to operational risk management. Naturally, the involvement of senior management in the formulation of the strategy is essential. The objective is to align the firm's risk profile (the risk that the firm wants to assume) with the selected risk appetite. The business objectives include targets like a market share or the introduction of new products and technology. Objectives are also stated for individual business units. The risk appetite does not only refer to the level of acceptable risk but also to the types of unacceptable risks. A risk map may be used as a quantifiable measure of the risk appetite that can be used to identify unacceptable risks.

The strategy also involves setting up an operational risk policy statement describing the overall approach and can be made specific to each business line as applicable. Policies often start with the objectives of operational risk management, which include increasing awareness and reducing operational losses. The statement of objectives can be complemented by a description of how the firm goes about the process and the agreed-upon definition of operational risk. The policy statement should also discuss the governance model and related roles and responsibilities. Also important are some general statements of risk management principles and a description of the expectations for the use of tools and reporting. For example, if there is a common self-assessment or database, the policy might state that every business area should implement it and maintain the information in an up-to-date manner.

In short, therefore, the strategy involves (i) setting effective operational risk policies and clear directions to follow, (ii) establishing an effective

management structure and arrangement to deliver the policy, and (iii) implementing the policy through an effective operational risk management system. The following section deals with the second component of the risk management framework, which is the process.

8.4 THE RISK MANAGEMENT FRAMEWORK: PROCESS

The process involves the day-to-day activities required to understand and manage operational risk, given the chosen strategy. The process consists of (i) risk and control identification, (ii) risk measurement and monitoring, (iii) risk control/mitigation, and (iv) process assessment and evaluation. Peccia (2003) adds two more elements: capital allocation and loss management. We will deal with the components (i)–(iv) in turn.

8.4.1 Risk and control identification

Risk identification starts with the definition of operational risk to provide a broad context for potential threats. The best way to identify risk is to talk to people who live with it on a daily basis, people who can be found in the support functional units or in the business lines themselves. Peccia (2003) suggests that identification should begin with a rigorous self-assessment of the exposures, the control environment and key risk drivers. He further suggests that risk identification should be based on a well-defined and consistent classification of operational risk, otherwise similar risks within different business lines or different times may be identified as being different, whereas different risks may be identified as being similar. The product of risk identification may be a risk map detailing which risks, and to what degree, apply to any one business, process or unit. The degree of risk is typically defined as frequency and severity, rated either qualitatively (high, medium, low) or on a quantitative scale.

Mestchian (2003) suggests a decomposition of operational risk management along the lines used to decompose operational risk into process risk, people risk, technology risk, and external risk. Thus, operational risk management can be decomposed into the following: (i) people risk management, (ii) process risk management, (iii) technology risk management, and (iv) external risk management. If this is the case, then risk identification may be reported as in Table 8.1 where people risk, process risk, technology risk and external risk are classified into low, medium and high according to business activities. Alternatively, a risk map may appear as in Figure 8.1, which shows the frequency and severity of the risk embodied in individual activities.

Table 8.1 Risk identification

	People	Process	Technology	External
Activity 1	L	M	M	H
Activity 2	H	L	M	H
Activity 3	M	L	L	M
Activity 4	M	L	M	M
⋮	⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮
Activity n	M	M	L	M

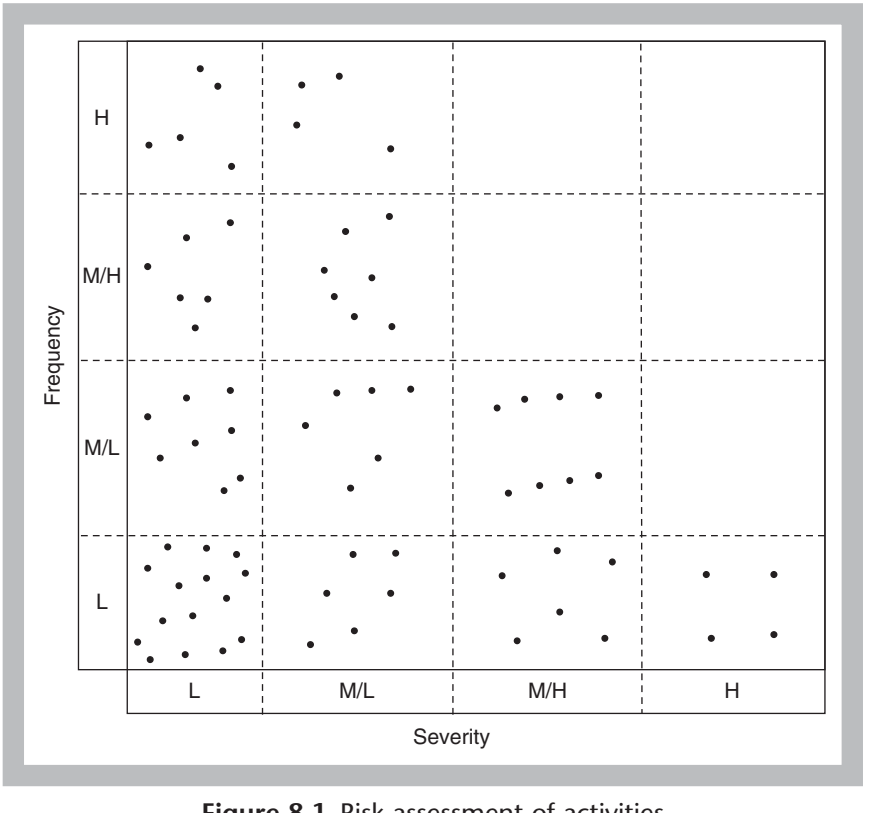

Figure 8.1 Risk assessment of activities

Risk identification should also include monitoring of the external environment and industry trends, as new risks emerge continuously, or it could be that risk may take on a new dimension. Internet security, privacy, patent risk, and discrimination are examples of risks that have increased dramatically over the past few years.

The identification of controls is part of the identification process, as it complements the identification of risk. Controls, a concept that we came across in Chapter 7, may reside at the business activity level, whereas others operate as part of the corporate risk management infrastructure. They include management oversight, information processing, activity monitoring, automation, process controls, segregation of duties, performance indicators, and policy and procedures. Risk mitigators include training, insurance programs, diversification and outsourcing. The control framework defines the appropriate approach to controlling each identified risk. Insurance, which is a means of risk control/mitigation, is typically applied against the large exposures where a loss would cause a charge to earnings greater than that acceptable in the risk appetite.

For the purpose of risk identification, the Federal Reserve System (1997) advocates a three-fold risk-rating scheme that includes (i) inherent risk, (ii) risk controls, and (iii) composite risk. Inherent risk (or gross risk) is the level of risk without consideration of risk controls, residing at the business unit level and is supervised through a review of significant activities. These activities are evaluated to arrive at the firm-wide inherent risk rating. Inherent risk depends on (i) the level of activity relative to the firm's resources, (ii) number of transactions, (iii) complexity of activity, and (iv) potential loss to the firm.

Composite risk (or residual risk or net risk) is the risk remaining after accounting for inherent risk and risk mitigating controls. The Federal Reserve System (1997) provides a matrix that shows composite risk situation based on the strength of risk management (weak, acceptable, strong) and the inherent risk of the activity (low, moderate, high). For example, when weak risk management is applied to low inherent risk, the resulting risk is low/moderate composite risk. On the other extreme, when strong risk management is applied to high inherent risk, the composite risk will be moderate/high. And when strong risk management is applied low risk, the composite risk will be low. Figure 8.2 provides an illustration of the Federal Reserve's classification of inherent and composite risk.

8.4.2 Risk measurement

As risks and controls are identified, risk measurement provides insight into the magnitude of exposure, how well controls are operating and whether exposures are changing and consequently require attention.

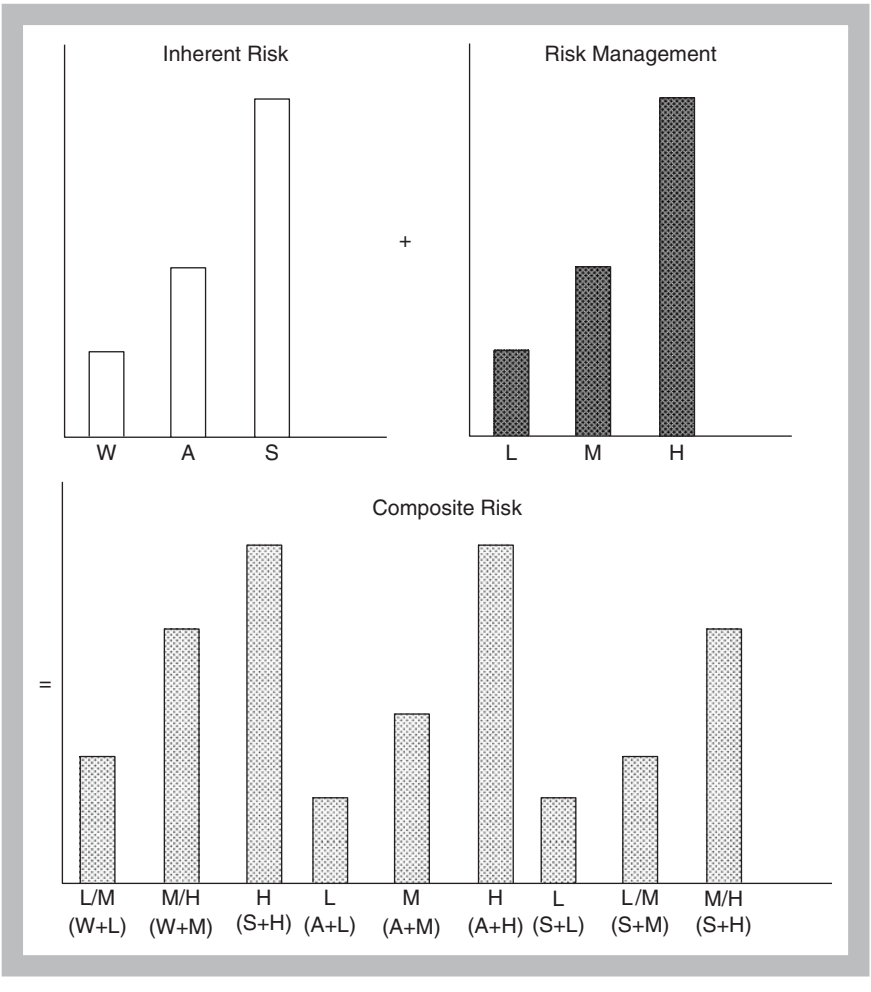

Figure 8.2 The Federal Reserve System's classification of inherent and composite risks

It remains true, however, that the borderline between identification and measurement is not well-defined and that there is some overlapping between the two. Haubenstock (2003) identifies the following items as relevant to the measurement of operational risk:

- Risk drivers, which are measures that drive the inherent risk profile and changes in which indicate changes in the risk profile. These include (as we have seen) transaction volumes, staff levels, customer satisfaction, market volatility, the level of automation. According to Crouchy (2001), risk drivers are associated with change (for example, the introduction of new technology and new products), complexity (of products, processes

and technology), and complacency (ineffective management of the business).

- Risk indicators, which are a broad category of measures used to monitor the activities and status of the control environment of a particular business area for a given risk category. The difference between drivers and indicators is that the former are *ex ante* whereas the latter are *ex post*. Examples of risk indicators are profit and loss breaks, open confirmations, failed trades and settlements and systems reliability.
- The loss history, which is important for three reasons: (i) loss data are needed to create or enhance awareness at multiple levels of the firm; (ii) they can be used for empirical analysis; and (iii) they form the basis for the quantification of operational risk capital.
- Causal models, which provide the quantitative framework for predicting potential losses. These models take the history of risk drivers, risk indicators and loss events and develop the associated multivariate distributions. The models can determine which factor(s) have the highest association with losses.
- Capital models, which are used to estimate regulatory capital as envisaged by Basel II.
- Performance measures, which include the coverage of the self-assessment process, issues resolved on time, and percentage of issues discovered as a result of the self assessment process.

Alexander (2003a) suggests three questions that are vital at this stage. These questions are:

1. What effect will the controls have on risk? For this purpose, a quantitative model is needed to relate risk to controls (a Bayesian network is recommended by Alexander).
2. Is it possible that by reducing one risk, another risk will increase? How can we quantify risk dependence, and how to control this dependence? Alexander argues that managing risk dependence is one of the main strengths of Bayesian networks.
3. What is the cost of controls, and is the likely reduction in risk worth the cost? This depends on the firm's utility function, which can be incorporated in the decision-making process.

Reporting is an important element of measurement and monitoring. Business lines perform the majority of data collection and reporting as part of their normal responsibilities. The central operational risk group adds value through benchmarking, analysis, and capital quantification. A key

objective of reporting is to communicate the overall profile of operational risk across all business lines and types of risk. The risk profile is represented by a combination of risk maps, graphical results, issues, and initiatives. Loss events are also reported to provide the historical database for risk analysis and quantification. There are two alternative ways of reporting to a central database as shown in Figure 8.3. One way is indirect reporting where there is a hierarchy in the reporting process, which can be arranged on a geographical basis. Otherwise, direct reporting is possible where every unit reports directly to a central database.

Risk assessment is a qualitative process that complements the measurement process because not all risks can be measured quantitatively. Checklists are probably the most common approach to self-assessment. Structured questionnaires are distributed to business areas to help them identify their level of risk and related controls. The response would indicate the degree to which a given risk affects their areas. It would also give some indication of the frequency and severity of the risk and the level of risk control that is already in place. The narrative approach is also used to ask business areas to define their own objectives and the resulting risks. The workshop

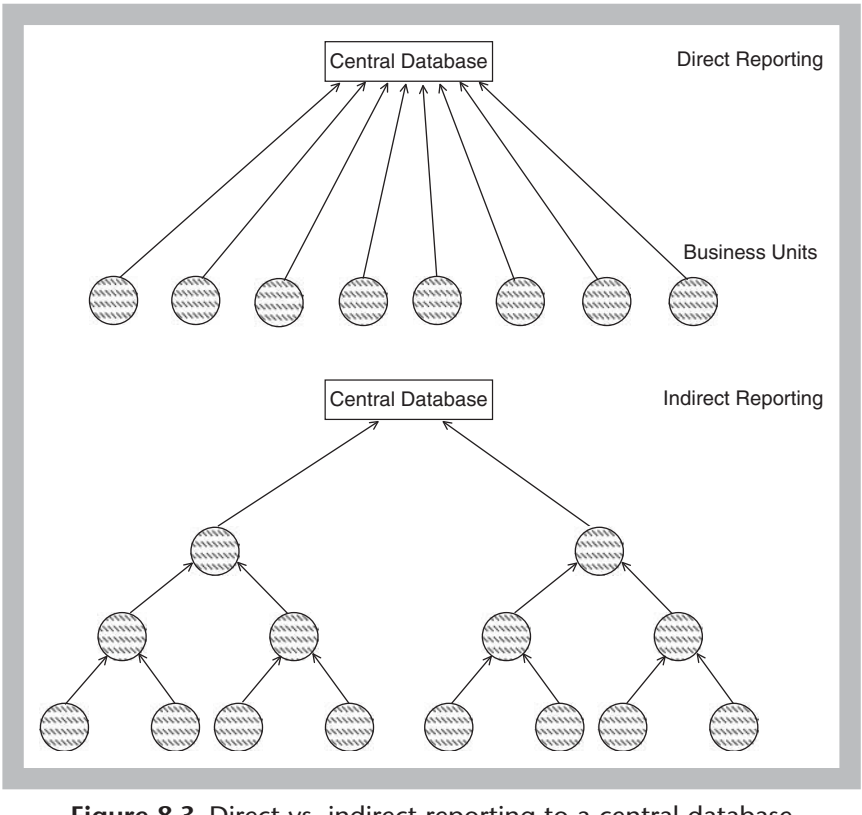

Figure 8.3 Direct vs. indirect reporting to a central database

approach skips the paperwork and gets people to talk about their risks, controls, and the required improvements.

Lam (2003b) argues for the use of elements of quantitative and qualitative approaches to the measurement of operational risk. In this respect, he identifies what he calls two schools of thought: (i) the one believing that what cannot be measured cannot be managed, hence the focus should be on quantitative tools; and (ii) the other, which does not accept the proposition that operational risk can be quantified effectively, hence the focus should be on qualitative approaches. Lam (2003b) warns of the pitfalls of using one approach rather than the other, stipulating that "the best practice operational risk management incorporates elements of both". Even the most quantitative experts of operational risk believe that a combination of quantitative and qualitative techniques and approaches is the way forward. For example, Chavez-Demoulin, Embrechts, and Neslehova (2006) admit that a full quantitative approach may never be achieved. However, they argue that some sophisticated techniques (such as advanced peaks over threshold modeling, the construction of dependent loss processes and the establishment of bounds for risk measures under partial information) are very powerful quantitative techniques.

Currie (2004) identifies what she calls "potentially unintended consequences" that arise from the use of operational risk models for practical risk management purposes. First of all, attempting to summarize all operational risk into a single measure could be "misleading and dangerous". The second consequence is that emphasis may be placed on the management of the model rather than reality. Currie argues that senior management may, on the basis of the model's output, take actions to reduce the model's estimate of operational risk rather than address the real core issues. There could also be misdirected focus and misdirected resources, the former with respect to the risks that can be quantified rather than major risks, and the latter with respect to the resources needed to maintain the model.

8.4.3 Risk control/mitigation

We now come to risk control/mitigation. When risk has been identified and measured, there are a number of choices in terms of the actions that need to be taken to control or mitigate risk. These include (i) risk avoidance, (ii) risk reduction, (iii) risk transfer, and (iv) risk assumption (risk taking). Sometimes, the notion of risk sharing is also suggested.

Risk avoidance can be quite difficult and may raise questions about the viability of the business in terms of the risk-return relation. Recall that the "most effective" way to eliminate the risk of rogue trading is to stop trading altogether. A better alternative is risk reduction, which typically takes the

form of risk control efforts as it may involve tactics ranging from business re-engineering to staff training as well as various less extensive staff and/or technical solutions. Reducing risk can raise a number of issues, including not only the risk-return relation of the activity but also the availability of resources. Cost-benefit analysis may be used to assist in structuring decisions and to prevent the business from being controlled out of profit. It is, therefore, a matter of balancing the costs and benefits of risk reduction.

Risk reduction can be illustrated with the aid of Figure 8.4, which shows a heat map by the business environment and the control environment. Suppose that the risk appetite of the firm allows it to be in the lowest three risk zones. This firm then attempts to move points (activities) falling in the high risk zones to the low risk zones by spending more money to strengthen controls (which may take the form of reduced return) and/or reducing the complexity of the business environment (if this is at all possible). Risk reduction may be represented, as shown in Figure 8.5, by a downward shift in the total loss distribution as a result of applying risk controls.

Risk transfer is what Mestchian (2003) calls "the external solution to operational risk". Insurance is typically described as a key tool of risk transfer, as some kinds of operational risk have been insured for some

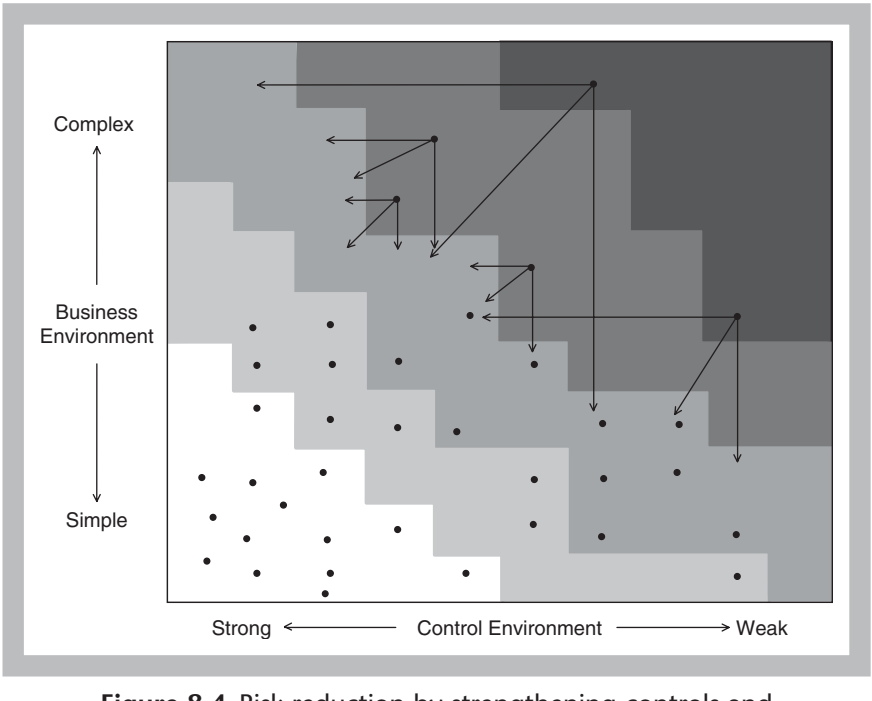

Figure 8.4 Risk reduction by strengthening controls and reducing complexity

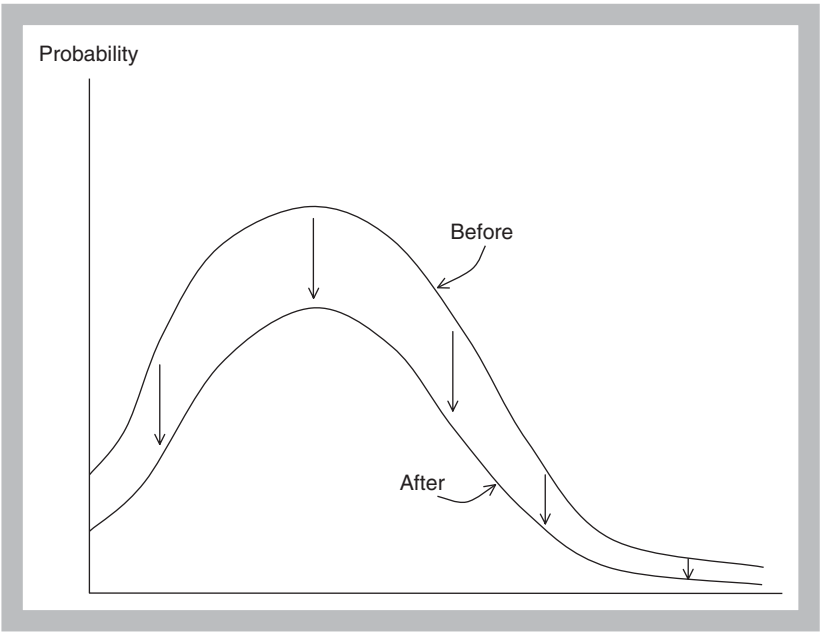

Figure 8.5 The effect of applying risk mitigators and controls on the total loss distribution

time. Examples include property coverage, fire, workers compensation, employers liability, and professional indemnity. Insurance provides firms with the means of taking risk off their balance sheets and avoiding the significant costs of capital associated with the provision for risk. Demand for insurance coverage has increased dramatically in recent times as senior executives have realized the consequences of operational risk. A special case of risk transfer is risk sharing, where the underlying idea is to transfer risk from individual firms to a group of firms participating in the risk-sharing scheme. One example of such a scheme is the so-called mutual self-insurance pools, which is regarded as an alternative to insurance, as we are going to see later in this chapter.

However, it is arguable that taking insurance does not really amount to risk transfer because the insured would still be exposed to risk. This is like saying that by insuring your house against fire, it is the insurer's house that will catch fire, not yours, even though the fire is on a street that is 20 miles away from the insurer's house!! Risk transfer in the strict sense would occur only if the bank outsources the activity to the insurer, which does not sound a good idea. Insurance merely provides financial cover, should risk bearing leads to losses. In this sense, insurance provides risk financing (specifically, external financing) rather than risk transfer.

Strictly speaking, therefore, a firm cannot transfer risk to an insurance company by taking insurance. However, an insurance company can transfer the risk of insuring another firm through reinsurance, whereas a firm can transfer the risk to another firm via outsourcing. We will have more to say about reinsurance later on, which allows us to concentrate on outsourcing here. Outsourcing enables firms to select the various business processes or functions that are non-core and high risk to a third party. Examples are the IT and HR functions. In addition to risk transfer, Mestchian (2003) argues that outsourcing has the following advantages: cost control, access to best practice tools and methodologies, freeing up capital and resources to focus on core business, and reduction in bureaucracy and administrative burden. The problem here is that transferring a specific operational risk may lead to the emergence of other operational risks (for example, legal risk invariably arises from outsourcing and insurance). A firm may choose to manage the risks that arise in the transfer process so that it achieves an overall net reduction in the risk profile. Again, it is a matter of balancing costs and benefits.

Opposite to risk avoidance is risk assumption, which is the action of taking on risk either through proactive decision or by default. In this case, the risk is supported by the firm's capital (hence, the Basel II Accord). In practice, a firm may use a combination of risk reduction, risk transfer and risk assumption, depending on the frequency and severity of the underlying risk. Figure 8.6 displays a risk map showing the zones where various actions are taken. A firm would therefore avoid high-frequency, high-severity risks, assume low-frequency, low-severity risks, transfer low-frequency, high- severity risks and avoid high-frequency high-severity risks. The question mark in Figure 8.6 represents the "grey" areas that, depending on the circumstances, can be reclassified to be in one of the four zones. Similarly, Figure 8.7 shows the distinction between expected loss and unexpected loss at a given confidence level. The expected loss, which is the mean of the loss distribution, is assumed. Unexpected loss can be severe (between the mean and a certain percentile corresponding to the confidence level) and catastrophic (above the percentile corresponding to the confidence level). Severe operational risk is typically covered by regulatory (or economic) capital, whereas catastrophic risk is avoided (if possible) or insured.

8.4.4 Process assessment and evaluation

The final step in the process component is assessment and evaluation, which is used to determine how well the firm is controlling and managing risk, the potential weaknesses, scope for improvement, etc. It is some sort of performance evaluation in relation to operational risk management,

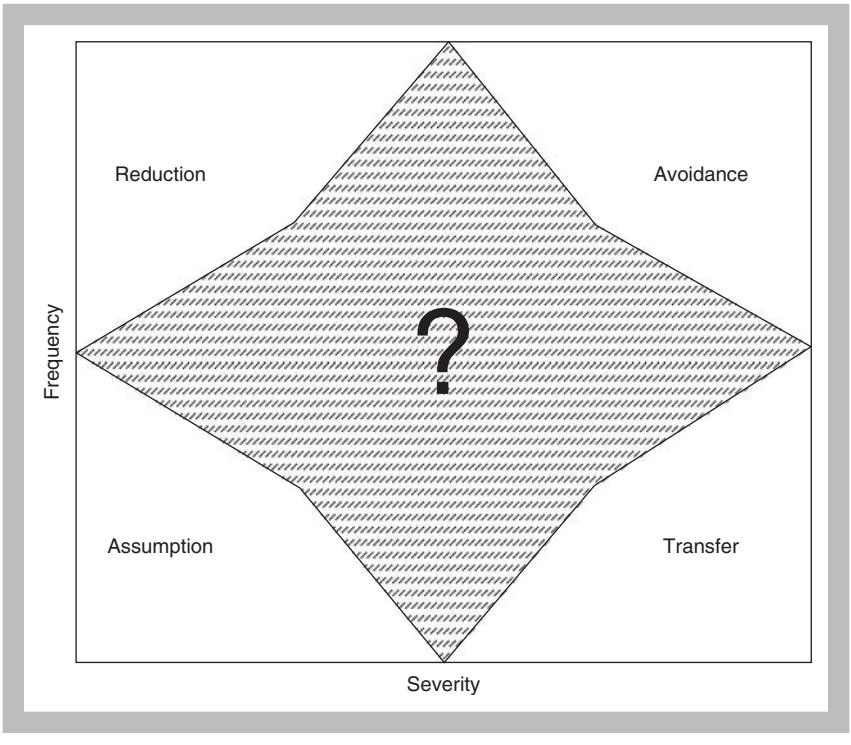

Figure 8.6 A risk map showing risk control/mitigation action

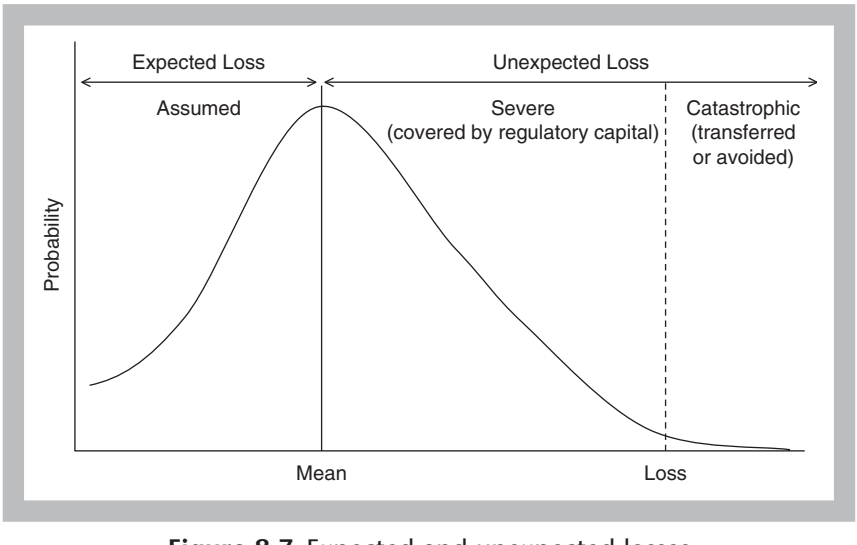

Figure 8.7 Expected and unexpected losses

where performance is measured against set standards to reveal when and where improvement is needed. This exercise also involves the measurement of the risk remaining after the risk controls and mitigation measures have been implemented. The amount of risk that remains is compared with the level of risk that the controls and mitigation were expected to achieve and also with the standards and objectives.

The internal audit function plays a role here, but as operational risk management becomes more explicit, the role of internal audit should change. In traditional models, the audit function is responsible for assessing controls, but now the primary responsibility for assessment is shifting to the business areas under the co-ordination of the operational risk management department. The role of audit should refocus on evaluating how well the overall risk management framework is functioning and on the testing of controls. Sharon (2006) argues that confusing the risk management function with the internal audit function amounts to confusing compliance with risk management and that merging the two essentially means that there is no oversight over the risk management function.

The role of the internal audit in operational risk management is made explicit by the BCBS (2004a). For example, one of the requirements for eligibility to use the standardized approach is effective risk management and control, in which internal auditors must regularly review the operational risk management process. In fact, banks are encouraged to establish independent internal audit and operational risk management groups in the structural hierarchy. The problem is that some firms place operational risk management within audit, claiming that it is the operational risk management department. However, Basel II suggests that for firms expecting (or required to) use the more sophisticated approaches, traditional decentralized business line management should be complemented by independent internal audit and corporate risk management departments. Kennett (2003) believes that there is perceived overlap of responsibility as far as the audit function is concerned. Audit, he argues, can feel threatened by the operational risk team, who may in turn view audit as being out of touch and not adding much value. Uncertainty about who is responsible for what leads to confusion and reduces the effectiveness of both. In an ideal world, they should be complementary.

8.5 THE RISK MANAGEMENT FRAMEWORK: INFRASTRUCTURE AND ENVIRONMENT

Infrastructure refers to the tools used to facilitate the entire risk management process, including systems, data, methodologies as well as policies and procedures. Mestchian (2003) refers to technology risk management by arguing

that all successful risk management projects share a strong emphasis on complete management of input data and computed results. Data in this sense include self-assessment data, internal event/loss data, operational data, and external loss data.

On the other hand, the environment refers to the surroundings that set the tone and behavior of the firm, including culture and external factors. Culture, which refers to the involvement and support of senior management and the related values and communication that set the tone for decision making, is a component of the process because it supports the risk management objectives. Culture is the set of shared attitudes, values, goals, and practices that characterize how a firm considers risk in its daily activities. Kennett (2003) argues that operational risk management becomes embodied in the culture of the firm, in the sense that every decision must involve an explicit review of the underlying operational risk. The environment is also about communications, accountability, and reinforcement. People are another component, as there should be adequate and trained people to do the job. The external component of the environment includes competitors, customers, regulators, the economy, and the law.

Hubner et al. (2003) discuss cultural drivers, suggesting that the experience of implementing credit and market risk management frameworks leads one to think that operational risk management will in time become an intrinsic part of a corporate culture. Incorporating awareness of operational risk into a firm's culture is an important part of prevention, so the question is how to promote this culture. This is why education and training are important. Because operational risk is present across the entire firm, every employee should be made aware of the issue and related management processes. There is a tendency to associate operational risk management with the control environment, which may make the framework appear as a source of additional bureaucratic burden. One thing that can be done is to include operational risk in performance measurement and in the basis of bonus calculation.

Mestchian (2003) discusses people risk management, suggesting that three sets of human factors affect operational risk, the first of which is that of organizational factors. Firms need to establish a risk management culture that promotes employee involvement and commitment at all levels. The culture should emphasise that deviation from established risk management standards is unacceptable. The second set is that of job factors, as mismatch between job requirements and an individual's capabilities strengthens the potential for human error. Finally, there are the personal factors, because people need to be matched to their jobs through appropriate selection techniques, taking into account such attributes as habits, attitudes, skills and personality. While skills and attitude can be modified by training and experience, others (such as personality) are difficult to modify.

8.6 WHAT MAKES A SUCCESSFUL RISK MANAGEMENT FRAMEWORK?

Swenson (2003) describes what he calls a "well-crafted corporate operational risk policy" as a policy that should strive to: (i) define operational risk and its components; (ii) identify the roles, responsibilities and interrelationships between the business units, internal audit, business line-resident risk management and firm-wide risk management; (iii) provide guidance commensurate with the size, complexity and the risk profile of the firm; (iv) document the process whereby risk self-assessment is completed; (v) establish templates for a risk-focused operational risk reporting package that includes risk and control self-assessment, key indicators and loss tracking; and (vi) address and/or cross-reference corporate and business activity guidance in selected areas (for example, loss escalation, separation of duties, and conflict of interest).

In general, a successful operational risk management framework requires the following:

1. Senior management support. Kennett (2003) argues that without senior management support, the operational risk team will "plough a lonely and ultimately unsuccessful furrow". After all, it is senior management that provides support, financially and visibly (for example, by ensuring that operational risk management is part of the appraisal process). Naturally, senior management needs to be persuaded that the operational risk management framework will deliver value. However, senior management support does not guarantee success (a necessary but not a sufficient condition for success).
2. The framework must be implemented in such a way as to provide direct value to the business units. Direct value may take the form of low regulatory capital, reduced losses, improved risk awareness, and the ability to price risk.
3. Incentives should be built into the system.
4. Consistency must be ensured in the system because it is the foundation for everything else that risk managers do. Consistency pertains to things like the definition of operational risk, risk categories, and key risk indicators.
5. The right people (in terms of right training, motivation and cultural fit) should be brought into the process.
6. The process should be dynamic, seeking improvement in measures and controls.
7. The results must be shared with all business areas.

8.7 THE ROLE OF INSURANCE IN OPERATIONAL RISK MANAGEMENT

Insurance has always been used to mitigate various kinds of operational risk, such as the risk of fire (damage to physical assets). As Young and Ashby (2003) put in reference to banking, "insurers have, for decades, played a role in financing the banking industry's operational risk by providing [insurance] products". Actually, insurance companies have been lobbying regulators to accept the idea of replacing (at least in part) regulatory capital with insurance or what they call the idea of "lightening the capital charge that banks must bear for operational risk".

8.7.1 Insurance products

Currently, a wide variety of insurance products (policies) are available to banks, which (as shown in Table 8.2) include peril-specific products (such as electronic computer crime cover) and multi-peril products (such as the all-risk operational risk insurance), as well as the traditional deposit insurance. The protection offered by an insurance policy is defined in terms of the maximum amount of cover and a deductible excess. Hadjiemmanuil (2003) considers in detail insurance and the mitigation of losses from legal risk and fraud.

Culp (2001) argues that the emergence of multi-peril products can be attributed to both demand and supply factors. On the demand side, these products provide a bank with a more comprehensive cover than the peril-specific products, which eliminates any gaps or overlaps that may exist when peril-specific products are used. They are also conducive to enterprise-wide or integrated risk management. On the supply side, the insurers benefit from the exploitation of risk correlations, which enables them to charge a lower price than the sum of the equivalent peril-specific products. There are, however, problems with the multi-peril products, such as the lack of critical mass and the lack of data. The lack of critical mass means that a large number of banks and insurance companies must be present for the product to be successful. Insurers need a large number of banks to spread risk, whereas a large number of insurance companies are required to spread the risk through reinsurance. The lack of data on all kinds of risk makes it difficult for insurers to assess the underlying risk and price the product correctly. Young and Ashby (2003) argue that the divergence of views on multi-peril products is like the S-shaped curve for the adoption of a new product, consisting of laggards, followers and early adopters. There are the skeptics, who question the viability of multi-peril products as a solution for operational risk; those who are indifferent, viewing multi-peril products as no more than an addition to the existing set of products; and the enthusiasts, who have already acquired the products.

Table 8.2 Operational risk insurance products

Product	Providing Cover Against
Fidelity/Banker's Blanket Bond	Employee dishonesty, fraud and forgery. Cover is also provided against office damage, in-transit loss and some forms of trading loss.
Electronic Computer Crime Cover	Computer failure, viruses, data transmission problems, forged electronic fund transactions.
Professional Indemnity	Liabilities to third parties for claims arising from employee negligence while providing professional services to clients.
Directors' and Officers' Liability	Expenses that might be incurred due to the legal actions arising from the performance of their duties.
Employment Practices Liability	Liabilities that may arise from infringements of the employment law, such as harassment, discrimination, and breach of contract.
Nonfinancial property	Property risks such as fire and weather.
Unauthorized Trading Cover	Unauthorized trading that is either concealed or falsely recorded.
General and other Liability	Public liability, employer's liability, motor fleet, etc.
All-Risk Operational Risk Insurance	Losses arising from internal fraud, external fraud, rogue trading, and many other forms of general liability.
Deposit Insurance	Losses incurred by depositors resulting from operational and non-operational risks faced by banks.

On the other hand, deposit protection schemes are typically government-run, as the government requires banks to acquire deposit insurance. Deposit insurance is not linked to a specific cause of bank failure, which makes it a multi-peril product in some sense. It is, however, rather controversial. On the one hand, consumer protection groups view these schemes as providing a "failsafe" for depositors against bank insolvency. Furthermore, Hadjiemmanuil (1996) argues that deposit insurance provides regulators with the option to refuse to bail out ailing banks, particularly if they are small or new. On the other hand, deposit insurance has been criticized severely, particularly by the proponents of free banking. For example, Karels and McClatchey (1999) attribute the high rate of failure of US savings and loans institutions in the 1980s to the use of "non-experience-rated, full-cover deposit protection schemes", which they explain in terms of moral hazard. In this case, moral hazard is manifested as the incentive for

insured depositors to place their funds in banks that take large risks in an attempt to offer high returns (Hadjiemmanuil, 1996).

8.7.2 The role and limitations of insurance

Leddy (2003) argues that the insurer's impact on risk management may be both direct and indirect. In the first instance, the insurer is likely to accept only good risks. Insurers also take into account distinguishing factors in pricing risks, thus forcing the insured to upgrade their risk management systems. He also identifies the steps of which the process of entering a contract with an insurer consists. These steps are illustrated in Figure 8.8. One advantage of insurance is that when a bank takes insurance, it can utilize the expertise of the insurer that covers many fields. Insurance also provides monitoring by the insurer on behalf of the stakeholders, including customers and the government. However, there are problems with insurance, starting with moral hazard considerations that may make it difficult or infeasible to insure low-frequency, high-severity events.

There are also doubts about the role of insurance. For example, one of the reasons suggested in Chapter 3 for the special importance of banks is their sheer size, which makes them too big for insurance companies, and hence they cannot use insurance effectively to cover all elements of

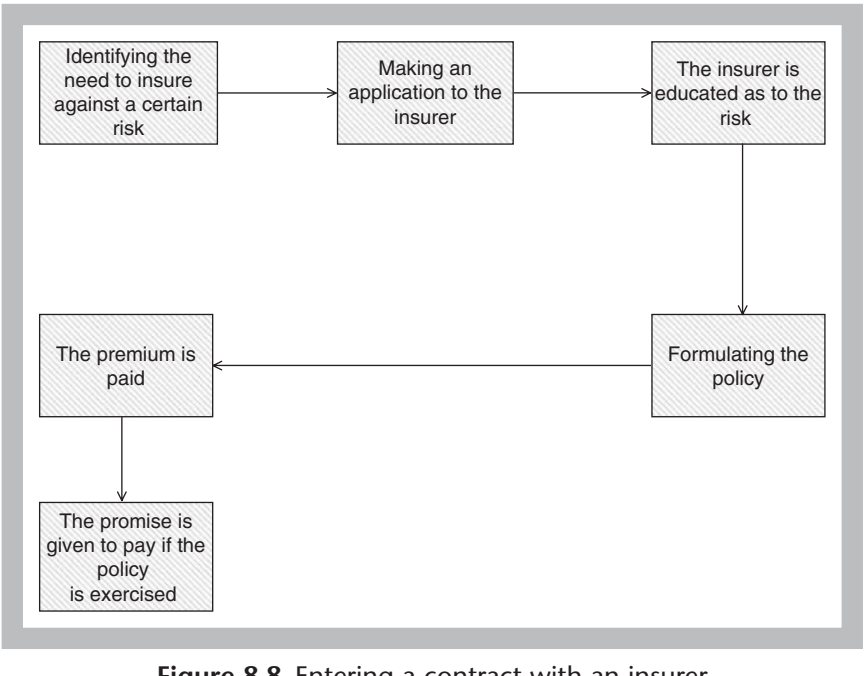

Figure 8.8 Entering a contract with an insurer

operational risk. Cruz (2003a) reiterates this point by arguing that the insurance industry is not well-capitalized vis-à-vis the banking industry, which makes a typical bank seeking insurance better capitalized than the insurance company. Furthermore, he identifies other pitfalls with insurance for operational risk, including the following:

1. Limiting conditions and exclusion clauses lead to doubt regarding payment in the event of failure.
2. Delays in payment could result in serious damage to the claimant.
3. It is difficult to determine the true economic value of insurance in the absence of sufficient and appropriate data.

Brandts (2005) casts doubt on the ability of insurance to provide a "perfect hedge" for operational risk, arguing that insurance compensation is often subject to a range of limitations and exceptions. Specifically, he identifies three problems (risks) with insurance. First, there is payment uncertainty resulting from mismatches in the actual risk exposure and the insurance coverage, as well as incompleteness of the compensation claims (insurance companies are notorious for telling customers that their latest mishap is not covered by the insurance policy). The second problem is delayed payment, which may result in additional losses. Third is the problem of counterparty risk resulting from the possibility of default by the insurance company.

Young and Ashby (2003) also cast doubt on the ability of the insurance products to go far enough in the current operational risk environment. The Basel Committee (BCBS, 2001b) has expressed doubts about the effectiveness of insurance products, stating that "it is clear that the market for insurance of operational risk is still developing". And although Basel II allows banks using the AMA to take account of the risk mitigating impact of insurance in their regulatory capital calculations, some conditions must be satisfied:

1. The recognition of insurance is limited to 20 percent of the regulatory capital held against operational risk.
2. The insurance providers must be A rated.
3. The insurance policy must have an initial term of at least one year and there must be a minimum notice period for cancellation or non-renewal.
4. There must be no mismatch between the insurance cover and the operational risk exposure.
5. Insurance must be provided by an independent insurer.

6. Banks must provide a documented insurance strategy.
7. Banks must disclose the extent by which regulatory capital has been reduced by insurance.

In general, regulators have a problem with the proposition that regulatory capital can be replaced (at least partially) with insurance. This is mainly because regulators are skeptical about the feasibility of immediate payouts (which is not what insurance companies are known for). There is also fear about the ability of the insurers to get off the hook (completely or partially) through some dubious clauses in the insurance policy.

Reinsurance, which is typically portrayed to be a means of spreading risk and the true means of risk transfer, has its own problems. Young and Ashby (2003) point out that the practice of reinsurance may create further problems for the insured, as it produces lack of transparency in the insurance industry to the extent that a firm holding an insurance policy finds itself dependent in recovering a claim on the weakest link in the reinsurance chain. The problem within insurance arising from payment delays may be accentuated by reinsurance, as an insurer or a reinsurer may not meet their obligations until they have secured payment from the next reinsurer in the chain. Reinsurance invariably results in the addition of further terms and conditions to the original insurance contract, again accentuating another problem of insurance. Reinsurance also creates counterparty risk that is unknown to the insured.

8.7.3 Determinants of the insurance decision

What determines whether or not a bank decides to acquire an insurance cover against operational risk? Some of these factors are bank size, the risk profile, the time horizons of managers/shareholders, and the attitude of stakeholders to risk and credit rating (Young and Ashby, 2003). The relation between bank size and the decision to insure is not clear-cut: small banks may be more inclined to acquire insurance than large banks because the former are more vulnerable to operational losses, a characteristic resulting from the fact that they do not have the spread of risks needed to pool the risk management benefits of insurance (Williams, Smith, and Young, 1998). On the other hand, a large bank might want to cover less-common, high-severity risks and may find it cost-effective to pass the day-to-day administration of common smaller risks to an insurer.

The risk profile affects the ability of a bank to acquire a cost-effective operational risk cover. As far as the time horizon is concerned, a longer-term horizon (of managers and shareholders) is more conducive to the acquisition of an insurance cover (Mayers and Smith, 1982). The effect of the risk attitude is clear, as risk aversion is more conducive to the acquisition of

insurance (Schrand and Unal, 1998). Finally, credit rating is a determining factor because a high credit rating is associated with a lower cost of debt financing, in which case a bank with a high credit rating may choose to protect itself against operational losses through borrowing rather than insurance (Doherty, 2000).

8.7.4 Alternatives to insurance

If insurance against operational risk is not viable, what are the alternatives? Young and Ashby (2003) suggest three alternatives: mutual self-insurance pools, securitisation and finite risk plans. A mutual self-insurance pool is a group of banks that pool in resources to cover the operational losses incurred by any member of the pool. The problem here is that banks typically think that they are better-run than the others, in which case they will not venture into a scheme like this.

The second alternative, securitization, is the use of derivatives to cover the risks that have traditionally been insured, such as the risk of weather-related losses (weather derivatives). One advantage of securitization is that the risk is (transferred?) to investors in the global capital market, which reduces the counterparty risk of the insurer. One possible means of securitizing operational risk is the creation of bonds similar to catastrophe bonds (see, for example, Lalonde (2005)). The problem here is that data on operational risk is so limited that the pricing of these bonds becomes a big problem. The third alternative to insurance is the finite risk plans, which are designed to help banks structure the financing of their retained risks, and so they are not comparable to insurance as such (Williams et al., 1998).

8.7.5 Incorporating insurance in regulatory capital

The last point to discuss in this section (and this chapter) is the incorporation of insurance as a risk mitigator in the calculation of regulatory capital as required by the Basel II Accord. In general, the effect of insurance can be calculated either separately or incorporated in a Monte Carlo simulation exercise. The first approach is suitable for the basic indicators approach and the standardized approach, which are not based on actual loss data. While this approach solves the problem of unavailability of reliable loss data, it has the problem of the neglect of potential overlaps or gaps in the insurance cover. The second approach is used with the AMA, which requires as a first step the mapping of loss events to insurance policies. This is important because a loss event may be covered by more than one insurance policy, whereas one insurance policy may cover more than one event type. Having done that, Monte Carlo simulations are conducted on gross losses to obtain a distribution of these losses.

Figure 8.9 shows 37 simulated gross loss observations and the effect of three insurance policies (or groups of policies) affecting certain loss events. It is assumed in this illustrative exercise that policy 1 affects loss events 1–24, policy 2 affects loss events 24–37, whereas policy 3 affects loss events 11–37. What is shown in Figure 8.9 is the compensation received form the insurer associated with various loss events (in no case is it assumed that any policy gives full compensation, hence the argument that insurance does not provide a perfect hedge against operational risk). When the effect of insurance is taken into account, net losses can be simulated as shown in Figure 8.10. The regulatory capital is calculated from the distribution of the net loss as described in earlier chapters.

Bazzarello et al. (2006) show formally how to incorporate the effect of insurance in an LDA model of operational risk by taking into account the AMA requirements that include: (i) appropriate haircuts reflecting the policy's declining residual term; (ii) the payment uncertainty due (for example) to mismatches between insurance policy coverage and the analyzed operational risk class; and (iii) the recognition of counterparty risk in the creditworthiness of the insurers and potential concentration of risk of insurance providers. The term "haircuts" reflects the requirement that the insurance policy must have an initial term that is longer than one year. This means that for policies with initial terms of less than one year,

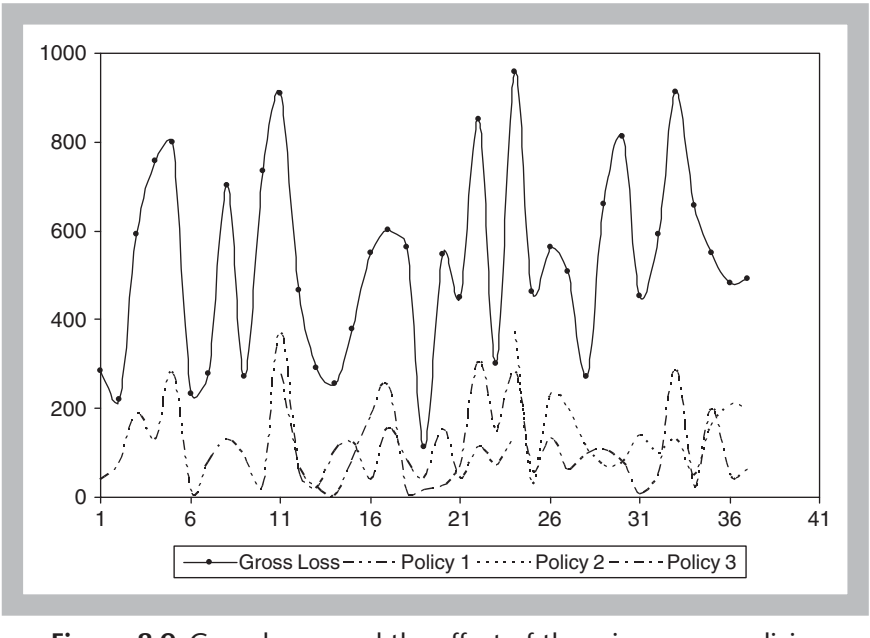

Figure 8.9 Gross losses and the effect of three insurance policies

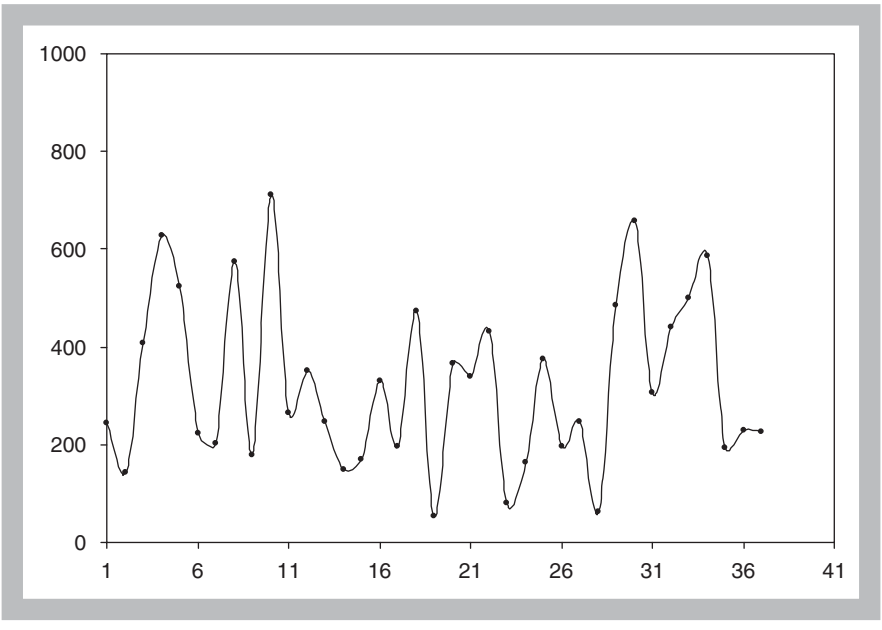

Figure 8.10 Net losses after the application of the insurance

haircuts should be introduced to reflect the shorter policy time horizon, up to 100 percent for policies lasting 90 days or less.

8.8 WHAT IS NEXT?

So far, we have covered aspects of Basel I and Basel II, then we moved on to the analysis of operational risk, starting with its description, definition and classification. Having done that, we moved on to the technical aspects of the topic, describing the general principles of modeling operational risk before going through a detailed description of the implementation of the AMA. In this chapter, we discussed the ultimate objective, which is the management of operational risk.

As we went through these topics, we came across a number of controversial issues that relate to operational risk as well as the Basel II Accord in general. What remains to be done is to come up with a view on the issues discussed so far in this book. This is the objective of Chapter 9, which starts with a recapitulation of the issues discussed in the previous chapters. Having done that, and before expressing a view on the Basel II Accord, the desirability (or otherwise) of banking regulation is discussed, since Basel II is a form of banking regulation.

CHAPTER 9

Summary and Conclusions

9.1 RECAPITULATION

In any study of operational risk, and the Basel II Accord that elevated it to explicit prominence, we are bound to encounter a number of critical questions pertaining to highly controversial issues encompassing a multitude of debatable topics. What we try to do in this chapter is to recount these questions, issues, and topics to find out how much we have learned by going through the previous eight chapters.

The issues that we intend to summarize our thoughts on in this chapter pertain to (i) the definition of operational risk; (ii) misconceptions about operational risk; (iii) the problems of modeling operational risk; and (iv) the pros and cons of Basel II, including the problems of implementation. These issues will be dealt with in separate sections. Then we consider the desirability or otherwise of Basel II as a form of banking regulation, which has been a controversial issue for a while. The final section of this chapter (and this book) presents some final thoughts.

9.2 DEFINING OPERATIONAL RISK: PICK AND CHOOSE FROM AN EXOTIC MENU

The official definition of operational risk adopted by the BCBS (which forms the basis of the regulatory capital requirements) is that it is "the risk of loss arising from inadequate or failed internal processes, people and systems or from external events". This definition is not universally acceptable and has been subject to criticisms, mainly because of what it includes

(for example, legal risk) and what it excludes (most notably business risk and reputational risk). The main feature of this definition is that it is based on pragmatism (to facilitate the measurement of operational risk) as opposed to comprehensiveness (including all risks arriving from the failure of people, processes, systems and external events). As a result of the historical development of this definition and the criticism directed at it, a large number of definitions have been suggested. An attempt has been made in this book to collect most of these definitions, which amounts to an exotic menu. Although attempting to pick the favorite "dish" out of this menu is hazardous, some comments are made on these definitions, as shown in Table 9.1.

Table 9.1 Definitions of operational risk

Definition	Comment
Any risk that cannot be classified as market risk or credit risk.	This is the negative definition of operational risk, which is hardly informative.
Uncertainty related to losses resulting from inadequate systems or controls, human error or management.	Are we mixing risk and uncertainty here? They are supposed to be different.
The risk encompassing all dimensions of the decentralized resources-client relationship, personnel, the physical plant, property and other assets, as well as technology resources.	The definition excludes external sources of operational risk.
Fraud, failures in controls and the like.	A definition that has the words "the like" can hardly be useful.
The risk arising from activities associated with fiduciary dealings, execution, fraud, business interruption, settlement, legal/regulatory and the composition of fixed costs.	Reference to "fixed costs" may imply that operational risk is one-sided, which is a disputable proposition.
All risks, other than credit and market risk, which could cause volatility of revenues, expenses and the value of the business.	Although this definition is somewhat negative, its strength is that it refers to costs as well as revenues, implying correctly that operational risk is two-sided.
A general term that applies to all the risk failures that influence the volatility of the firm's cost structure as opposed to its revenue structure.	This definition again implies that operational risk is one-sided.

(*Continued*)

Table 9.1 (*Continued*)

Definition	Comment
The risks associated with human error, inadequate procedures and control, fraudulent and criminal activities, technological shortcomings, and system breakdowns.	No mention of external factors, which can cause massive operational losses.
The direct or indirect loss resulting from inadequate or failed internal processes, people and systems, or from external events.	This is probably the broadest and conceptually most correct definition of operational risk. One weakness of the BCBS's definition of operational risk is that it excludes indirect losses.
Operational risk is the risk of operational loss.	This must be the least-informative definition.
The risk associated with operating a business.	This definition is rather vague and perhaps inaccurate. Market risk and credit risk are also associated with operating a business.
The risk that there will be a failure of people, processes or technology within the business unit.	No mention of external factors.
Every type of unquantifiable risk faced by a bank.	Describing operational risk as "unquantifiable" is controversial and the antithesis of the AMA.
A loose-limbed concept that includes potential losses from business interruptions, technological failures, natural disasters, errors, lawsuits, trade fixing, faulty compliance, fraud and damage to reputation, often intangible fallout from these events.	Perhaps the word "diverse" is more appropriate than "loose-limbed".
The risk that deficiencies in information systems or internal controls will result in unexpected loss.	This definition excludes the risk arising from the failure of people and from external events.
The risk that a firm will suffer loss as a result of human error or deficiencies in systems or controls.	Unlike the previous definition, this definition includes human errors but excludes external factors.
The risk run by a firm that its internal practices, policies, and systems are not rigorous or sophisticated enough to cope with untoward market conditions or human or technological errors.	A rather comprehensive definition.

(*Continued*)

Table 9.1 (*Continued*)

Definition	Comment
The risk of loss resulting from errors in the processing of transactions/ breakdown in controls/errors or failures in system support.	No mention of external factors.
The risk that the operation will fail to meet one or more operational performance targets, where the operation can be people, technology, processes, information, and the infrastructure supporting business activities.	No mention of external factors.
The risk of business disruption, control failures, errors, misdeeds, or external events, and is measured by direct and indirect economic loss associated with business interruption and legal risk costs, and also by "immeasurable" such as reputation risk costs.	A rather comprehensive definition.
The excess of allocation of capital in the firm after market and credit risk capital have been eliminated.	The problem with this definition is its implication that the absence of capital allocation means the absence of risk.
The uncertainty of loss in the book value of the firm due to failures in the manufacturing of the firm's goods and services.	A rather restrictive definition.

Having gone through the menu of definitions, it may not be that hard to pick the worst definition, which is that operational risk is the risk of operational loss. This is no more than describing water as water, as an old Arabic proverb says. A view on the issue of defining operational risk that seems to make sense is that being too fussy about the definition of operational risk does not serve any purpose. Right, provided that the definitions that tell us nothing useful are excluded.

9.3 THE PROBLEMS OF MEASURING OPERATIONAL RISK

One of the definitions of operational risk, as every type of unquantifiable risk faced by a bank excludes the possibility of measuring operational risk, casting doubt on the feasibility of implementing the AMA. Sometimes, difference is made between the measurement and assessment of operational risk on the grounds that measurement is a quantitative exercise whereas assessment is a qualitative exercise. A middle-of-the-road view on

this issue is that both approaches must be used to get a feel of a firm's exposure to operational risk.

If we discard the extreme views that operational risk cannot be measured, the problems associated with the measurement of operational risk can be stated as follows:

- The absence of a universally-acceptable definition of operational risk.
- The scarcity of hard loss data and the subjectivity of soft data (external loss data or those obtained from scorecards and scenario analysis).
- The cyclicality of loss events, which casts doubt on the feasibility of extrapolating the past to measure future risk.
- The difficulty of assessing the level of correlation between operational risks of different kinds and/or those arising in different business lines.

These are the problems associated with the AMA, which require measuring operational risk by modeling it (basically fitting a distribution to operational losses). As crude as they may appear to be, no such problems arise in the case of the less sophisticated basic indicators approach and the standardized approach. So, do we forget completely about the measurement of operational risk because of these problems? An attempt will be made to answer this question in the final section of this chapter.

9.4 MISCONCEPTIONS ABOUT OPERATIONAL RISK

Operational risk is frequently portrayed to be one-sided, idiosyncratic, indistinguishable, and transferable via insurance. These arguments are disputable and can be discarded without much effort. This is how:

- Operational risk is not one-sided in the sense that there is no risk-return trade off. One-sidedness means that bearing operational risk could result in losses but it produces no returns. This is nonsense, as no firm will bear any kind of risk if there is no anticipation of return. Financial institutions bear the risk of rogue trading because trading is profitable. Firms in general bear the risk of fire in conducting their daily business because the conduct of daily business brings in profit.
- Operational risk is not idiosyncratic in that it affects only one firm and not other firms in the system like credit risk. This is a rather strange view, given that the very establishment of the Basel Committee came as a result of the Hersttat Bank crisis: one bank's failure, as a result of an operational loss event, adversely affected many banks world-wide. Operational risk is definitely not idiosyncratic, particularly in the banking industry where banks do a lot of business in the interbank market.

This, however, does not mean that every operational loss event experienced by a firm affects other firms in the industry.

- Operational loss events are not indistinguishable from credit or market loss events. What matters is the cause of the loss, not how the loss is incurred. If a trader breaches trading guidelines, then a market downturn produces losses, this would be an operational loss event (not a mixture of operational and market loss events). If there is no breach of trading guidelines (and other operational failures), then it is a loss associated with market risk.
- Operational risk cannot be transferred through insurance. A bank taking insurance against rogue trading will not transfer the risk of rogue trading to the insurance company unless the bank outsourcers its trading activity to the insurance company, which does not make any sense. Insurance provides (external) risk financing, not risk transfer.

9.5 THE PROS AND CONS OF BASEL II

Basel II has been described as "probably the most ambitious regulatory reform program any group of regulators has ever attempted". It is definitely an improvement over Basel I in that (i) it includes a more sophisticated measurement framework for evaluating capital adequacy; (ii) it provides incentives for better corporate governance and fostering transparency; (iii) it deals explicitly with operational risk; (iv) it is more risk-sensitive than Basel I; and (v) its application would narrow the gap between economic capital and regulatory capital. However, the Accord has been subject to severe criticism that can be summarized in the following points:

- Risk measurement depends heavily on the VAR methodology, which has been found to be unreliable and destabilizing.
- VAR-based regulatory regimes (including Basel II) may lead to lower systemic risk at the cost of poor risk sharing, an increase in risk premia and other adverse consequences. Furthermore, the reduction in systemic risk may not materialize if too many firms are left outside the regulatory regime.
- Reliance on credit rating agencies is misguided.
- Operational risk modeling is problematic (as we saw in a previous section).
- Basel II will exacerbate procyclical tendencies, making the financial system more susceptible to crises. Business cycles will be more severe