The Virtues of Operational Risk Management

Ariane Chapelle[1]

Université Libre de Bruxelles
Solvay Business School
Centre Emile Bernheim

October 2005

Abstract

After a short review of the rules of Basel II regarding the treatment of operational risk, this paper focuses on four axes of operational risk management: static analysis of losses with incident databases; dynamic analysis of losses with dashboards and loss ratios; key risks and performance indicators, and finally, risk and control self-assessment. This contribution, based both on academic research and on professional experience, has the double objective of demystifying the management of operational risk, as well as emphasising its importance.

Prof. Ariane Chapelle
Université Libre de Bruxelles CP 145 / 1
Avenue Roosevelt, 50
1050 Brussels
Belgium
Tel. : +32.2.650.48.71
e-mail : ariane.chapelle@ulb.ac.be
home page : www.solvay.edu/cours/chapelle

[1] I am grateful to Yves Crama, Georges Hübner, Jean-Philippe Peters, and the members of the Risk Management department of ING Belgium, for their precious collaboration on these questions. I also thank the participants of the conferences : EFMA, Investance, Leaseurope BNB and the 3rd International Finance Conference for their helpful comments on earlier versions of this paper.

1. Introduction

For the first time in the field of banking regulation, the Basel Committee on Banking Supervision, in its reform commonly named "Basel II", recognises operational risk as a specific risk category for banks to cover by regulatory capital, along with credit risk and market risk.

Operational risk is defined as "*the risk of losses resulting from inadequate or failed internal processes, people, and systems or from external events. The definition includes legal risk, but excludes strategic risk and reputation risk.*" (BIS, 2003).

This definition includes seven types of risks that may be categorised into three different types of issues : fraud, security, and processes.

Fraud includes both internal and external fraud that is, breach, thefts and unauthorised activities perpetrated either by the members of the financial institutions themselves, or by outside agents. Security includes both physical assets security, with damage to physical assets and workplace safety, as well as IT security, such as control of hacking attempts, confidentiality and data integrity. Processes, broadly speaking, regroup namely the types of events falling into the "Clients, Products and Business Practices" category, including losses incurred following a bad execution of information or legal requirement in a commercial relationship with a client. The event type "Execution, Delivery and Process Management" targets all types of errors that occur when processing, transmitting, and classifying internal, external, or commercial data in the course of business.

The Basel Committee acknowledges the potential magnitude of operational losses for banks and recognises the need to cover those risks with capital. The Committee's "rule of thumb" has been to allocate around 12% of the total regulatory capital to operational risk. Parallel to this, regulators clearly stated that the global capital requirements would not increase with the reform (BIS, 2003).

Two questions can be raised at this point : can we reasonably state that the safety of the banking sector will increase with the Basel II reform if we only shift regulatory capital across risks, without modifying the global requirements? Next, is regulatory capital the proper answer to operational risk supervision? This paper addresses both of these questions by attempting to show the potential positive impact of an efficient, organised, operational risk management approach.

The paper is structured as follows : section 2 shortly summarizes the Basel requirements regarding operational risk measurement and management, section 3 reviews the former banking practices regarding operational risk and section 4 presents an approach for operational risk management structured in four axes. Section 5 concludes.

2. The Basel II Requirements

In line with the regulatory treatment of credit risk, the first pillar of Basel II for the measurement of operational risk capital proposes three approaches:

- the *Basic indicator approach* (BI): the operational risk capital is defined as a multiple (15%) of the gross income of the institution, under the hypothesis that risk is related to

size. Gross income is the sum of the interest margin, the fee income, and the other revenues. This most simple approach is only available to local banks.

- the *Standardised approach* (BI): similarly to the first approach, the operational risk capital is calculated on the basis of gross income, but a split is made per business line. The regulator distinguishes different operational risk levels according to the type of activity performed. Subsequently, the multiple of gross income varies from 12% for the least risky business lines (Retail Banking, Retail Brokerage, Asset Management) to 18% for the riskiest ones (Corporate Finance, Trading and Sales, Payment and Settlement), with an intermediate level at 15% of gross income (Commercial Banking, Agency Services) .
- The *Advanced Measurement Approach* (AMA) : banks are free to model the calculations defining the necessary regulatory capital covering their operational risk themselves, with a confidence interval of 99.9%. This sophisticated approach is strongly recommended for banks that are internationally active. In order to adopt the AMA, banks have to comply with numerous quantitative and qualitative criteria regarding their risk management tools, techniques, involvement and expertise in the field of operational risk. Among those :
  - incident reporting history of 5 years, with a minimum of 3 years;
  - existence of contingency and business continuity plans;
  - independent ORM function;
  - implication of senior management;
  - written policies and procedures;
  - inclusion of external data for the calculation of the capital at risk, along with scenario analysis and stress testing;
  - active day-to-day OR management.

Incident reporting is the most basic requirement of the Basel agreement, the key element in risk identification. Incident data collection is paramount for sound practices in operational risk measurement and monitoring. In order to comply with the AMA, banks are required to have an incident database of minimum three years' history on day one of the reform, that is, January 1, 2007. This means that they need to have started to collect their loss data last January 2004 at the latest.

Statistically, however, it is far from demonstrated that internal incident reporting is sufficient to assess the economic capital needed to cover for operational risk. Indeed, economic capital should be sufficient to cover operational losses in 99.95% percent of the cases. In order to have a reliable value-at-risk measure, one must assess the full distribution of operational losses, including rare events. But since internal reporting databases cover rather short periods of time, they are very likely to be exempt of rare events, or, if they are not, the bank might have gone bankrupt before it could report such an incident.

For this reason, external events data have to be added to the internal database. External events are large losses incurred by members of the banking sector over about the last decade. Several databases (like Opvantage) and consortia of banks (like ORX) are built for that purpose. Since the first publications of the Basel Committee on Operational Risk, several groups of banks have come together to build and share a collective database of large events, in order to model the right-hand side of their loss distribution.

Loss distributions aggregate two distinct distributions : the *severity* distribution, representing the losses per event, and the *frequency* distribution, modelling the number of losses per period of time. The loss distribution for operational risk is asymmetrical, skewed to the left, with a long tail to the right. Put another way, the mass of the losses are of high frequency and low severity, while increasingly large losses become more and more rare. External data fall into the category of "low frequency, high severity" data. Their impact is very significant on the tail of the distribution, and on the value-at-risk calculations of the regulatory capital, set at 99.9% confidence interval.

Here is what could be called "paradox of incident data collection": regulators' requirements regarding internal operational loss reporting are strict, while it is in fact the external data that determine most of the amount of regulatory capital. Furthermore, the type of external data included, the cut-off mix of internal data versus external data, and the modelling choices have significant impacts on the results.

Although fascinating, the econometric issues of operational risk modelling are far beyond the scope of this paper. Many contributions already address those questions. For a summary overview of those questions, see for instance Frachot et al. (2001). The difficulties linked to the optimal mix of internal and external data to model the distribution are addressed in Frachot et al. (2002), in Chapelle et al (2004 and 2005). For general issues on operational risk modelling see Alexander (2003) and Cruz (2002).

If large incidents drive the regulatory capital amount, why impose full incident reporting? For one main reason : risk management. Know your losses, know the frequency, the place of occurrence, identify the causes and the recurrent breaches in your control framework, and you will manage your operational risks properly. Incident reporting is the core of the operational risk management process. It is the foundation on which a comprehensive operational risk management (ORM) is based.

3. Operational Risk before Basel II

If the regulatory framework is new for operational risk, this is not true for operational risk management itself. Banks and financial companies have managed their operational risks for ages. Long before regulators talk about operational risks, internal and external fraud were monitored and reprehended by the inspection department, the security department, or by internal audit.

Besides fraud, internal auditors and internal controllers are dedicated to risk identification and prevention within the different departments of the bank. They make sure that policies and procedures are properly designed and effectively applied. Information Technology (IT) departments and IT controllers are very attentive to preventing breaches in information system security, guaranteeing data integrity and protecting websites from hacking attempts. In order to protect the continuity of activities in case of a major system breakdown or physical event, Business Continuity Plans have been set up and tested in most large financial institutions.

Nevertheless, since the Basel reform, operational risk is now seen as a comprehensive well-identified risk management activity, as is market risk or credit risk management. The new Basel agreement has for the first time put a common name on a myriad of practices already existing in banks. Shedding light on existing heterogeneous practices, the Basel requirements

for operational risk management and supervision provide a powerful incentive to better organise and to expand this activity.

Since the first publication of the Basel Committee on operational risk, a growing literature on this new area of research has started flourishing. Academics, consultants and practitioners have entered the field with great enthusiasm. While modelling issues are usually addressed by academics or by research departments within banks, management issues are often the focus of consultants, gathering the best practices of the sector, or by bankers themselves, willing to share their professional experience. Several books review some of the best practices in risk management in banking (Crouhy et al., 2001), or more specifically in operational risk management (Hoffman, 2002).

Despite its heterogeneous nature, operational risk monitoring and assessment can be organised using key approaches and techniques, making it possible to comprehend and easy to communicate throughout the organisation and, therefore, easily manageable. One of the possible ways to organise the various aspects of ORM is presented in the section below.

4. Operational Risk Management in Practice

Beyond the rules and the modelling requirements for measuring the regulatory capital required to properly cover operational risk, the Basel Committee acknowledges a particular attention to the management of this risk. Illustrating this concern is the document entitled "Sound Practices for the Management and Supervision of Operational Risk" published by the Committee (BIS, 2002), fully integrated to the first pillar and mandatory for all banks, regardless of the complexity of the risk measurement approach. This section is dedicated to the practices described in this document.

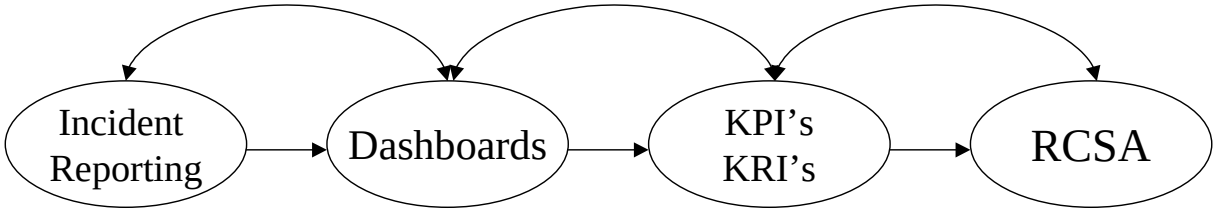
Operational risk management serves essentially two goals : the avoidance of catastrophic events, and the reduction of medium and small losses. Some techniques are efficient to serve the first goal, while others better serve the second. This section will describe them both.

Several types of organisation of risk management can be found in the literature. Here we will structure our approach in four dimensions, from the most static one to the most proactive one, each of them being an input for the following. This structure is presented in figure 1.

The four dimensions are the following :

1. *Incident Reportin*g : static analysis. It gives a cartography of past events, their nature and their cause.
2. *Dashboards* : dynamic analysis. They describe the evolution of operational events by activity or by department, providing a dynamic representation of the losses.
3. *Key Risks Indicators (KRI's) / Key Performance Indicators (KPI's)* : benchmarking analysis. They allow a comparison of the dashboards to predefined standards and an assessment of the evolution of the risk.
4. *Risk and Control Self Assessment (RCSA)* : proactive analysis. It provides a prospective view of the potential risk based on the collection of information by experts in the field.

Figure 1. The Four Dimensions of Operational Risk Management (ORM)



4.1. Incident Reporting

Incident reporting is the core of ORM. It is the first step in identifying the losses within an organisation. Summary statistics first display frequency and severity data by event type and by business line, according to the regulatory categories. If this is undoubtedly needed for compliance purposes, it might be not the best tool for the risk management of a financial institution, having a different structure or nature of activities. A more useful set of summary statistics will match the organisation chart of the financial institution, bank, or company that uses its database. It will split amounts by department, by people in charge, or by geographical zone of activity. For a bank retail network for instance, the reporting may be split by bank branch, and, or by type of client.

Even before detailing the frequency and the severity of each type of loss, incident reporting in an organisation or in a department should first display the total loss amount caused by operational events. Such a simple measure, long neglected and sometimes never measured in financial institutions in the past, may provide a powerful tool to raise awareness on operational risk within an organisation

Next, the analysis can identify the "low severity, high frequency" losses and the "high severity, low frequency" losses, with the remaining events. Both need further investigation, since they can be the symptoms of serious breaches in control within the organisation.

One of the key criteria in operational risk management is whether a possible loss is capped or not. That is, in case of an operational event, the potential loss amount is limited by any type of control. Examples of measures to cap potential losses are maximum amounts allowed by the IT system for a given type of transaction, or maximum cash values held in a branch because of the possibility of hold-ups, etc. Capping potential losses is, and should be, a main concern for senior management.

To that extent, rare events of large amounts are the first candidates in the identification of uncapped risks. When the incident database includes abnormal amounts of losses, these require individual investigations in order to accurately identify the circumstances that led to such losses.

Likewise, recurrent minor losses require further investigation, at least once. They might also be the consequence of an effective cap of losses in an activity highly exposed to operational risks. This is typically the case of a manual activity, as in mutual funds administration, or in payment processing. Operational losses due to processing errors are frequent but limited due to effective control procedures and systems design. But recurrent losses could also be a more

worrying symptom of a systematic breach in control or in process that lead to systematic or frequent losses, with possibly very large amounts at stake.

An incident database is a view of the operational losses in an organisation that can provide, if interpreted correctly, a list of priority controls and investigations to be performed. Database analysis provides the facts, but does not identify the risks. This belongs to other dimensions of ORM. The evolution of losses, globally and per category, is better performed by operational dashboards, as described in the following subsection.

4.2. Dashboards

After the identification of losses comes monitoring with the help of dashboards. They need to be specifically designed for each type of activity, and common activities should have similar dashboards, to allow for comparison. Dashboards come from a specific analysis of the incident database, providing an organised view of losses and their evolution in the various places of the organisation. They are a powerful way to communicate the extent and the evolution of these losses, and therefore provide management with a first image of the potential risks.

Efficient dashboards are concise focused on the pieces of information that are directly useful to the manager. They allow the manager to have a global view of its losses in a glimpse. Simple summary statistics are usually enough to provide relevant view of the situation : number of events, sum of losses, max, min and average amount of losses, evolution over time, comparison with similar activities. The figure 2 provides an example of a dashboard for a commercial bank.

Figure 2. Example of a Dashboard

DPT	**ALL EVENTS**				
	Number	**Amount**	**Average**	**Loss/Income %**	**TOP 5 amounts**
Q 1					**1.**
Q 2					**2.**
Q 3					**3.**
Q 4					**4.**
					5.
	BY EVENT TYPE				
	Type x				
	Number	**Amount**	**Average**	**Loss/Income %**	**TOP 5 amounts**
Q 1					**1.**
Q 2					**2.**
Q 3					**3.**
Q 4					**4.**
					5.

Quarterly reporting is generally enough. Except for the largest operational back-offices, where the risk is naturally higher, monthly reporting might overload managers. The number of losses reported, along with their amount, synthesise the two key dimensions of operational risk : *frequency* and *severity*.

A “loss/income ratio” (LIR) provides a most efficient tool to capture the attention of the manager : it measures the value lost due to operational events, in proportion of the profit of the department (in case of cost centers, this loss amount can be compared to the total costs).

This measure is derived from the same concept as the « *loan/loss ratio* » that is often used in credit risk management, expressing in basis points the amount lost in defaulted credits as compared to outstanding credit. The « *loss /income ratio* » (LIR) has the double advantage of being based on a well-known notion which is therefore easy to communicate, and constituting a useful means of comparison of operational risk performance across departments and activities.

The dashboards allow two types of comparison :
- across time for a single department,
- simultaneous, for several departments of a similar nature

The first axis will provide managers with useful information regarding the evolution of losses and risks. It also provides a feedback for the risk management measures that have been put in place. The second axis is only applicable to similar activities, various retail bank branches.

But what are the acceptable limits to losses? What are the acceptable ratios? Dashboards alone don't provide an answer to this question. In order to have a benchmark, one needs to add Key Risks and Performance Indicators to the analysis.

4.3. Key Risk Indicators and Key Performance Indicators

The third dimension of ORM opens the way for the prospective analysis of operational risks, with the introduction of key risk indicators specific to each type of activity. It also introduces a benchmark in the assessment of operational risk exposure with key performance indicators, also tailored per activity. Even though both these indicators have theoretically different roles, in practice they are often merged into performance indicators.

Each department or service will thus dispose of its own set of indicators, specific to the nature of its tasks, the degree of automation, the process organisation and the financial flows involved, just to name a few criteria. For instance, back-offices of dealing rooms will have indicators such as the number of front-office / back-office reconciling items, the amount of overdue interest charge, or the number of trade fails ; the IT department will have the amount of downtimes, the number of hacking-attempts, and project-planning overruns.

At this level of sophistication of reporting, one has to bear in mind that the collect of information can be significant, and may not, depending on the existing reporting system in place, be worth the cost it incurs. In this dimension of ORM more than in others, a cost-benefit analysis of the risk monitoring should be made before setting up such a system in an activity.

Risk indicators are particularly appropriate in the activities concentrating the largest amount of financial flows (typically dealing rooms) or in activities where points of reference in the risk assessment are lacking. Those should be on the priority list for the implementation of key risk and performance indicators.

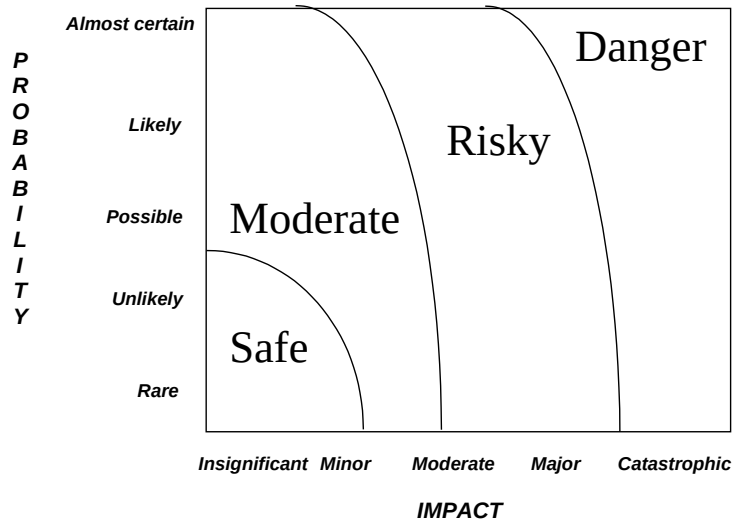
In terms of risk assessment, the acceptability of a risk level for a given activity depends, to a large extent on the risk appetite of the institution and on the level of errors and events the organisation is ready to accept, depending for instance on the strategic importance of the activity in question. If the limit threshold is exceeded, the manager is asked to increase or improve the level of controls.

4.4. Risk and Control Self-Assessment (RCSA)

The last dimension of ORM, according to our structure, is the most proactive one. RCSA is based on the idea that people on the field are better informed than external auditors or controllers. The Basel Committee has indeed acknowledged this fact, by allowing banks to model their risks themselves, provided the comply with a number of criteria. Thus, the RCSA gives the floor to the line manager as well as to key, experienced people in the assessed activity or entity.

The RCSA process is a co-operative work between line management, operational risk management, and internal audit. In workshops and group discussions, the objectives are to identify the various risks of the entity, assess the level of control, and suggest improvements. To this end, a frequency / severity matrix is certainly a great help to guide the discussion (Figure 3).

Figure 3 : Frequency / Severity Matrix



The two axes of this graph correspond to the two characteristics of a risk : frequency and the severity. The likelihood of occurrence of the potential risk is measured on the vertical axis, while the potential impact is measured on the horizontal axis. The gradation is voluntarily qualitative, to reflect the fact that these notions can be adapted to the scale of the analysis : a major impact for a single department might be seen as minor at the scale of the entire organisation, for example. Impact can be measured proportionally to the profits – or the costs – of an entity. Likelihood may also by adjusted to the scope of the matrix : yearly, monthly, daily... depending of the size of the activity.

The matrix can be divided into zones of growing level of risk that will call for an increasing need for controls or actions. Each element on the graph represents a possible operational event. Events falling into the « safe » zone do not deserve particular attention from the management, while those falling into the “danger” zone - which should be empty - require immediate action.

Bear in mind that this matrix includes potential incidents given the controls that are already in place. Indeed, without any internal control, one could almost place every incident in the « danger » zone. Thus, incidents placed in the « safe » zone are probably events mastered by efficient controls and procedures.

When the risk level exceeds the limit threshold defined by the management, three types of measures can be taken :

- *improvement of internal controls* : this comprises a broad range of measures, among which the reorganisation of the manual processes, increased task monitoring, employee education …
- *risk transfer* : when the risk is harder to reduce, management may decide to transfer it to another entity, either another department merging different activities, or an external party, typically an insurance company ;
- *risk avoidance* : in extreme cases, the risk of an activity can only be suppressed by closing down the entity – or the people - generating this risk.

5. Conclusion

After a short review of the legislation, this paper has essentially focused on the principal axes of operational risk management in a model of four successive actions, with an increasing degree of proactivity in the approach to risk.

This contribution, mixing academic research and professional experience, has the double objective of demystifying the management of operational risk, as well as of emphasising its importance.

The Basel reform will not increase the global requirement of regulatory capital, even though it refines its measurement. Everything, or almost everything, relies on the quality of risk management : comprehensive, efficient, concrete. Describing it was our purpose.

6. Bibliography

- Alexander, C., (2003): Operational Risk: Regulation, Analysis and Management, FT Prentice Hall, London.
- Bank of International Settlements, (2002)« Sound Practices for the Management and Supervision of Operational Risk », Basel Committee on Banking Supervision.
- Bank of International Settlements, (2003): “The New Basel Capital Accord", Consultative Document, Basel Committee on Banking Supervision.
- Bank of International Settlements (2004), “International Convergence of Capital Measurement and Capital Standards – a Revised Framework”, Basel Committee on Banking Supervision, June.
- Chapelle, A., Y. Crama, G. Hübner and JP Peters (2004), « Basle II and Operational Risk: Implications for risk measurement and management in the financial sector », in *Efficiency and Stability in an Evolving Financial System*, BNB-NBB Conference, Working Paper BNB-NBB n° 51.

- Chapelle, A. G. Hübner et JP Peters (2005) *Le risque opérationnel : Implications de l'Accord de Bâle pour le secteur financier*, Cahiers Financiers, Edition Larcier, January, 155 p.
- Crouhy, M., Galai, D. and Mark, R. (2001): Risk Management, McGraw Hill, New York.
- Cruz, M. G. (2002): Modeling, Measuring and Hedging Operational Risk, Wiley Finance, New York.
- Frachot, A., P. Georges, and T. Roncalli (2001): "Loss distribution approach for operational risk", Working Paper, Groupe de Recherche Opérationnelle, Crédit Lyonnais.
- Frachot, A., and Roncalli, T. (2002): "Mixing internal and external data for managing operational risk", Working Paper, Groupe de Recherche Opérationnelle, Crédit Lyonnais.
- Hoffman, D. G., (2002): Managing Operational Risk: 20 Firmwide Best Practices Strategies, John Wiley & Sons Ed., New York.