Cultural Risk and Risk Culture: Operational Risk after Basel II

Roman Buchelt
Stefan Unteregger

Prologue

"When anyone asks how I can best describe my experience in nearly 40 years at sea, I merely say, uneventful. Of course there have been winter gales, and storms and fog and the like, but in all my experience, I have never been in any accident of any sort worth speaking about. I never saw a wreck and never have been wrecked, nor was I ever in any predicament that threatened to end in disaster of any sort."

E. J. Smith

After two million sea miles logged and 26 years of commanding passenger ships, Edward John Smith knew exactly what it was that sounded comforting to passengers. He was considered experienced, highly capable and enjoyed an excellent reputation as the "Millionaire's Captain," and today we would not attach any importance to what he said had he not been the captain on the maiden voyage of the *Titanic,* which, as is generally known, had been acclaimed as practically unsinkable until it went down after hitting an iceberg, taking the lives of 1,500 passengers and crew members – including that of the captain.

Why the *Titanic* sank is a topic of discussion to this very day, but it seems as if a chain of errors and inadequacies were the cause, as is often the case in catastrophes of this dimension. First of all, the myth that the ship was unsinkable led the captain to navigate too fast and too carelessly through iceberg waters. Furthermore, the safety measures were inadequate – only half as many places in lifeboats as passengers on board (and even so this was more lifeboats than required by the regulations). Other reasons were poor emergency planning and drills, and above all, a lack of discipline – many lifeboats could not be lowered to the water fast enough or were half empty because passengers simply refused to get in.

Thus, the entire incident appears to be the outcome of the failure of interrelated factors: *people* (the crew, and also the passengers), *systems* (the ship including all of its equipment) and *processes* (emergency plans and procedures) triggered by an *external event* (the iceberg). These are precisely the four classical causes of what is called *operational risk,* which we will look at more closely in the following. At the end of that fateful night of April 15, 1912, the *Titanic* lay at the bottom of the North Atlantic Ocean as it were like a punishment for the arrogance of its builders and operators, reduced to the bitterly and dearly learned lesson that not to know one's risks (or refusing to see them) does not necessarily mean that there are no risks.

Banks' Operational Risks

Banks are not unsinkable either, though of course, when they go down this usually does not involve the loss of human life, but still, the comparison of some banking risks with those of maritime navigation is far-fetched only at first sight. It is not only the fact that many concepts used in risk management come from the maritime insurance industry, the essential meaning of the term *operational risk* is much closer to the original meaning of risk (from the Italian *rischio,* Spanish *risco* = a cliff) than is true for the other risks of the banking business. We do not necessarily need to use an analogy of the *Titanic* to see that organizational structures and responsibilities, process design, system analysis, emergency planning, etc. are not only effi-

ciency-enhancing or merely perfunctory measures in running a business but also represent essential risk factors, specifically the risk factors of operational risk.

Operational risk is definitely not something that can be ignored: for most banks, it may be much greater than market risk and constitutes the second-largest risk category after credit risk. As illustrated by some spectacular cases in the past ten years, these risks can cause a bank to suffer major losses. The loss, for example, in the Schneider case in Germany in 1994, in which some 50 banks had granted excessive loans due to inadequate credit auditing and loan approving procedures, totaled over DEM 2 billion. At the Japanese Daiwa Bank, a single trader lost USD 1.1 billion in speculative dealings over a period of 11 years by taking advantage of a much too broad scope of competence and by engaging in illegal and unauthorized trading. Even the renowned Barings Bank with its 200-year old history was driven into bankruptcy by one clever gambler; its losses totaled USD 1.4 billion.[1])

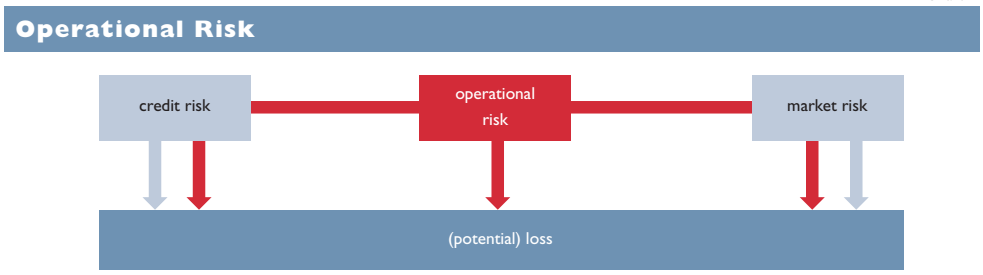
This list could go on forever, but what has actually hoisted the concept of operational risk to a risk category in its own right has been – apart from such illustrative examples of operational losses in the recent past – the increasing intrinsic complexity of the banking business fostered by the advent of (and dependence on) the blessings of information technology, new and changing fields of business, growing globalization and automation as well as the emergence of increasingly complex products. As the measurement of credit risk becomes more and more sophisticated, the capital cushion available for softening the other risks is flattening. For this reason the Basel Committee for Banking Supervision found it necessary and (in contrast to reputational or strategic risk) feasible to have a separate view of operational risk.

However, it is apparent that the nature of operational risk and thus also the requirements on how to deal with this type of risk are very different from the classical risk categories of market and credit risk. It may very well be justified to speak of cultural risk in this context, considering that we are dealing with a highly varied and interrelated set of risks with different origins when referring to the overarching term of operational risk. In other words we are looking at the corporate culture, or more precisely, at the risk culture, which essentially is the way a company conceives risk and implements risk management in daily business. The management of such a ubiquitous risk, which is at the same time so hard to grasp, is an essentially managerial task. It must be performed on a broad organizational basis with support from the executive board and through efficient communication.

It is one of the characteristics of operational risk that it may already exist within a bank (and it usually does) before credit risk occurs or market risk is incurred. The difference between operational risk and other risks is the fact that credit and market risks are business risks specific to the banking industry in contrast to operational risk as a general business risk or more precisely, operating hazards, which, however, also have particular features

1 *Description of the Barings and Schneider cases are contained in Utz (2002), as regards Daiwa see Brandner et al. (2002).*

Chart 1



Operational risk may materialize directly or indirectly through credit or market risk.

in the banking business. Whether or not a loss event is to be classified as an operational loss event is not determined by the consequences of the event but rather by the cause(s). Operational risk may materialize directly or indirectly through market or credit risk. In this context, we would like to mention as an example all transactions carried out with fraudulent intent (like at Daiwa and Barings) in which a market risk generated a loss (price loss or variation margin payments) but the cause was an operational risk (deficiencies in the organization and processes, fraud). The losses in the Schneider affair, in contrast, were caused by nonperforming assets, which apparently represents a typical case of credit risk; but in fact operational risk was at the root also of this case (deficiencies in credit auditing and loan approving procedures).

To identify the causes as described above is the only rational way to arrive at a definition of operational risk that allows a differentiation from other risk categories (see chart 1). Although the negative definitions of operational risk as everything that is not credit or market risk, which had been common practice for a long time, do indicate to a certain extent what might be meant, they are hardly suitable for precisely defining the scope; neither are definitions with a focus on certain technical risks (such as those used in information technology) which, by ignoring interdependencies, do not capture the full extent of the given risk potential. On the basis of the already mentioned four causes, we will look at the Basel approach to solve the problem of the definition in the next section.

It is clear that even before the application of the term operational risk to banks (it is a term taken from nuclear technology just like MCA or maximum credible accident), banks in practice devoted particular attention to specially risk-exposed areas. Ever since the beginning of banking, people have been aware of the temptation that such an accumulation of assets constitutes for persons with a criminal inclination (within and outside the bank), but the risks of external events (fires, flooding and other natural disasters) are also just as old as any type of business activity.

However, technological progress created new types of dependence and thus potential threats, ranging from the issue of energy supply, which grew in significance at the same pace as the influence of information technology increased, to electronic data processing with its seemingly inexhaustible potential for errors and breakdowns of all types. In this context, decision-makers also finally grasped the fact that employees are prone to make more mistakes, the more complex their tasks are.

Generally, long before the advent of Basel II many credit institutions had already put in place the most varied set of control mechanisms and procedures as well as defined responsibilities to manage those vulnerabilities that could not be summarized under the uniform concept of a risk category but nonetheless had to be avoided. The sum of these procedures was a great step forward towards the establishment of an operational risk management system, and for this reason we would like to describe them briefly.

To counter physical threats, very extensive security and safety measures have become commonplace (security glass, access controls, fire alarm and extinguishing systems, preventive measures against theft and robbery), supplemented by operating instructions and security rules. Insurance policies are also widely used in this area. The design and documentation of efficient workflows that are the least prone to error is usually the task of a specialized *organization department* whose job typically includes monitoring processes, identifying problem areas and eliminating them by optimizing workflows. The organization department sometimes includes the area of *information technology* unless it has been set up as a separate organizational unit or the main tasks of electronic data processing have been outsourced to a subsidiary or other IT center used jointly with other institutions. This area covers all data security measures as well as the management of access rights and system availability in accordance with the requirements of the specific areas and quality assurance in the development of in-house software. The *legal department* is entrusted with the highly specialized task of tracing and eliminating problems and hindrances that may result from statutory or contractual obligations and of preventing damages from occurring through unclear – and in some case even illegal – contractual provisions. The *internal audit department* serves as another control layer, supplementing workflow rules and management responsibilities. Its task is to discover and eliminate deficiencies and sources of errors and it is also responsible for monitoring the "human factor."

We therefore can see that not only had some of the vulnerabilities subsumed under the concept of operational risk already been taken into account – at least to a certain extent – by banks long ago, but especially that currently the responsibility of monitoring, controlling and mitigating these risks is distributed across the entire structure of banks. Thus, it is crucial for banks to implement and integrate an operational risk management system.

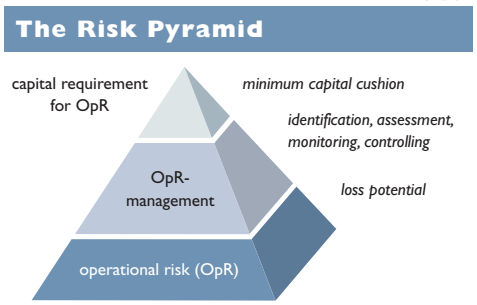
The Basel Rules on Operational Risk

The central element of the Basel II rules on operational risk is the definition of this risk category by the Basel Committee on Banking Supervision as *"... the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic or reputational risks."*[1]*)*

This definition covers the main risk factors dealt with in the previous section; the definition rests purely on the causes, which, considering the nature of operational risk, is an optimal

1 *See BIS (2003).*

Chart 2



Capital requirements are a capital cushion that will only work if they rest on the efficient management of operational risks.

approach and methodologically very sound. Moreover, the Basel Committee's definition coincides in many areas with other definitions that have evolved internationally, except for the fact that the main risk factors may have been assigned different names and weightings. Thus, for example, the Group of Thirty adds the factor of management error as a separate item to the list of failures of people and processes[1]) to specifically point out the dire consequences of errors of judgment at the highest level, while the Association of German Public Sector Banks (Bundesverband Öffentlicher Banken Deutschlands, VÖB) explicitly mentions catastrophes in addition to external events.[2]) Nonetheless, the Basel definition very well covers the central aspects of operational risk; it should also be noted that it explicitly mentions legal risk and clearly delimits operational risk from strategic and reputational risks. It is also worth mentioning from a historic point of view that the original definition[3]) still spoke of the ". . . risk of direct or indirect losses . . .," but was then shortened and put into the wording mentioned above, which leaves less room for interpretation.

The definition of operational risk is very important because, on the one hand, it sets it apart from other risk categories and, on the other hand, forms the basis for the treatment of operational risk ranging from raising awareness at the management level to the calculation of capital requirements. We would like to use a pyramid to illustrate this point.

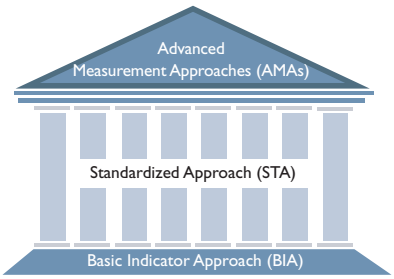
The base of the pyramid is made up of the operational risks inherent in a bank's activities, products and infrastructure; the bank must be aware of this fact to be able to take effective measures to limit these risks. As illustrated above, procedures and control mechanisms are already in place at this level in the various areas, which have been designed specifically for certain types of risks and certain risk aspects. Acknowledging these facets of operational risk, as it permeates the entire bank and cannot be allocated to one specific area, is the first step in developing a risk culture with the ultimate purpose of establishing a comprehensive and consistent operational risk management framework.

Such a risk management framework is the next step in the pyramid, the middle section. This level is where the central control and coordination of all efforts occur; this is the only way to avoid loopholes, redundancies or conflicts relating to scopes of competence which might undermine the efficiency of risk management procedures. A central office is necessary in order to keep an eye on the overall interaction between the areas and any coordination problems that may arise, a task that is not feasible at the level of divisions or departments.

1 *See van den Brink (2001). The publications of the Group of Thirty are available at http://www.group30.org*
2 *See VÖB (2001).*
3 *See BIS (2001).*

Chart 3

The Basel Approaches for the Calculation of the Operational Risk Capital Charge



Even the control mechanisms available to management, which it needs to comply with its statutory responsibilities, can only be guaranteed by implementing a comprehensive risk measurement and reporting system.

The top of the pyramid and also the decisive innovation of Basel II for operational risk management is doubtlessly the capital cover for losses arising from operational risk. In the first draft[1]) of the new capital adequacy framework, the Basel Committee was still skeptical about the usefulness and enforceability of capital requirements for operational risk (as a subgroup of what is termed "other risks"), but ever since the second consultative paper it has become firmly anchored in the document. Currently, there are three approaches to determining the amount of capital required to cover operational risk; these approaches are progressively more complex and are supported by increasingly just as complex application requirements (see chart 3).

The Basic Indicator Approach (BIA) computes the capital charge directly as a percentage (alpha factor, $\alpha = 15\%$) of the bank's average total gross income for the past three years. Thanks to its simplicity, this approach is easy to apply; its weakness, however, is that the indicator is hardly risk sensitive and may moreover contradict overall banking management objectives. Although higher income may indicate that it has been earned by taking greater risks, these will hardly be limited to operational risks, i.e., only the indirect effect of operational risk is taken into account. Neither would this approach reward banks that apply operational risk management (e.g. risk mitigation measures). According to the Basel Committee, internationally active banks and banks with major operational risks should select an approach commensurate with their risk portfolios, in others words, not the Basic Indicator Approach.

One step up is the Standardized Approach (STA), which distributes the average gross income of the past three years across eight prescribed lines of business (corporate finance, trading and sales, retail banking, commercial banking, payment and settlement, agency services and custody, asset management, retail brokerage). For each of these lines of business, a beta factor has been defined, which, depending on the degree of risk, is 12%, 15% or 18% and is applied like the alpha factor of the BIA, but only to the gross income of each of the respective business lines. The capital requirement results from the sum of the capital requirements of all lines of business. By making a differentiation between the more and the less risky lines of business, the Standardized Approach achieves a somewhat better risk sensitivity than the Basic Indicator Approach; however, it does not reward operational risk management measures either.

The most complex methods of calculation are the Advanced Meas-

1 *See BCBS (1999).*

Chart 4

Methodologies of Calculation, Complexity and Risk Sensitivity of the Basel Approaches for Operational Risk

Capital requirement for OpR (K) in the various approaches.

urement Approaches (AMAs), which is actually the umbrella term for all loss data-based, quantitative-statistical methodologies that banks will be permitted to use in the future to calculate the capital requirements for operational risk.

As such approaches are currently still being developed and to date no standardized method has emerged, the Basel Committee intends to give banks the widest scope possible in defining their methods as long as they rest on a sound methodological and quantitative foundation. This is why the Basel Committee does not give any further details of possible approaches but states as main types of approaches of this group the Internal Measurement Approach (IMA), the Loss Distribution Approach (LDA) and the Scorecard Approaches (SCA). All AMAs have in common that they add the dimension of classes of potential loss event types to the classification of standardized lines of business of banks in order to incorporate internal loss data and external loss data of the bank in a methodologically meaningful way. Internal Measurement Approaches combine event probabilities and average losses computed using loss data and risk indicators for each business line/event type combination in order to calculate the capital charge; the Loss Distribution Approaches model loss distributions by line of business and risk event type based on historic loss data; Scorecard Approaches attempt to control the amount of an initially determined capital requirement by using qualitative features as well as, for example, threshold values for quantitative indicators.

The implementation of an AMA requires relatively great methodological and monitoring efforts, but this makes the procedures accordingly risk-sensitive, i.e., their results can be used directly to control operational risk. Furthermore, at present only banks applying an AMA are permitted to factor to a limited extent operational risk-mitigating measures (insurance contracts) into capital charges.

Sound Practices for the Management and Supervision of OpR

The Sound Practices paper outlines a set of principles that provide a framework for the management and supervision of operational risk. These ten principles are phrased in general terms and are intended to be applicable to all banks regardless of their individual environment. Thus the Basel Committee was able to summarize the discussion as it stands today and, in light of the increasing significance of operational risk, to create a foundation for further work. The first three of the ten principles are dedicated to the establishment of a management environment for operational risk:

(1) The board of directors should be aware of the major aspects of the bank's operational risks as a distinct risk category and should participate in the further development of the risk management framework. This framework should be based on a firm-wide definition of operational risk and lay down the principles of how to identify, assess, monitor, control and mitigate operational risk.

(2) The internal audit function should monitor and assess the operational risk management framework, but it should not be directly responsible for operational risk management.

(3) Senior management should ensure the consistent implementation of the operational risk management framework throughout the entire banking organization as well as the definition of the necessary responsibilities, guidelines and procedures.

The following four principles detail the requirements of risk management:

(4) Banks should identify and assess operational risk in its entirety, especially when new products, activities, processes or systems are introduced.

(5) Banks should regularly monitor operational risk profiles and material exposures to losses; there should be regular reporting of pertinent information to senior management.

(6) Banks should install policies, processes and procedures to control and/or mitigate operational risks. Banks should periodically review these strategies.

(7) In the event of severe business disruptions, banks should have contingency plans and business continuity plans in place to ensure their ability to operate on an ongoing basis.

On the role of supervisors:

(8) Supervisors should require that all banks, regardless of size, have an effective framework in place to identify, assess, monitor and control/mitigate material operational risks.

(9) Supervisors should conduct regular evaluations of a bank's policies related to operational risk management; they should ensure that there are appropriate mechanisms in place which allow them to remain apprised of developments at banks.

The last principle refers to disclosure requirements:

(10) Banks should make sufficient public disclosure to allow market participants to assess a bank's approach to operational risk management.

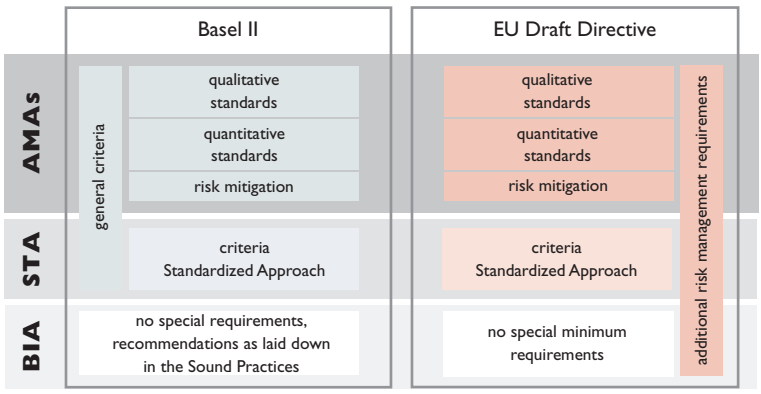
Although Basel (i.e. the third consultative paper) does not make the Sound Practices directly binding, their influence on the application requirements described in the following is clear.

When introducing an approach to calculating operational risk charges, the middle section of the risk pyramid, i.e., operational risk management in the widest sense, is given special attention as also shown in the *Sound Practices for the Management and Supervision of Operational Risk*[1]) published by the Basel Committee on Banking Supervision (these overarching principles were developed gradually from the working papers of the Basel Committee of 1998[2]) and are considered a minimum standard for operational risk management owing to their general significance – see box). Thus, the actual introduction of one of the approaches described in the New Basel Accord is formally contingent on the fulfillment of the

1 *See BCBS (2003).*
2 *See BCBS (1998a, 1998b).*

Chart 5

Comparison of the Planned Application Requirements of the Approaches Under Basel II and the EU Draft Directive



application requirements which, in a modified form, are included also in the provisions of the current draft Directive of the European Union.

There are no binding application requirements for the Basic Indicator Approach defined in the framework of the Basel draft; however, it does strongly recommend that banks apply the *Sound Practices for the Management and Supervision of Operational Risk* when calculating operational risk capital charges.

The current Basel consultative paper sets out common general criteria for banks to qualify for the use of the STA and AMAs, such as the involvement of the board of directors and senior management, the establishment of a conceptually sound risk management framework and the availability of sufficient resources to implement the framework. Additionally, separate criteria are formulated specifically for the STA and the AMAs, some of which elaborate in more detail the principles of the *Sound Practices.* In the case of the AMAs, these criteria are grouped into qualitative and quantitative standards, with the former basically elaborating on the principles contained in *Sound Practices,* while the latter are guidelines for data quality and the statistical-methodological implementation of the approaches. All application standards have in common that a credit institution may not use the STA or the AMAs to calculate operational risk capital charges unless all of the pertinent requirements have been met.

The proposals in the current draft of the European Union Directive follow a similar train of thought; here as well there are no separate criteria defined for use of the BIA but a catalogue of criteria for the application of STA and detailed qualitative and quantitative standards for AMAs (instead of common general criteria for the STA and AMAs, those criteria that apply to both approaches were included in both cases for the sake of clarity). However, we would like to stress the additional risk management requirements laid down in Annex I of the working document, which define, irrespective of the approach selected, i.e., also for the BIA, certain minimum standards for operational risk management. On the one hand, these are in Section 1 of the Annex in the form of general requirements for risk management, which also apply, of

course, to operational risk, and on the other hand, in Section 7 with the special requirements for operational risk.

The middle section of the pyramid shown may by no means be disregarded even in the case of BIA and STA, although the requirements grow more sophisticated the greater the complexity of the approaches and thus in the case of AMAs, also call for the highest qualitative and quantitative standards. Because of the low risk sensitivity of the two simpler approaches it is all the more important to incorporate risk analysis methods and quantitative measures into the overall operational risk management framework. Thus, banks can reap the benefits of higher risk awareness and, as a consequence, risk prevention. Unless this is accomplished, the notion of having done everything necessary to control/mitigate operational risks by holding the calculated capital charge could turn out to be a dangerous delusion. There is no doubt about the Basel Committee's view of the significance and especially of the close relationship between the framework for operational risk management and the calculation procedures for the applicable capital charges: *"The qualifying criteria are minimum standards . . . that a bank must meet in order to avail itself of a particular regulatory capital assessment methodology. The supervisor may well wish to use the supervisory review process to assess compliance with these criteria, but they form an integral part of the first pillar."*[1])

Aspects of Operational Risk Management

The nature of operational risk is very complex, and one of its features is that it is often unconsciously incurred. It is all the more difficult and important to actively identify risks and to develop a culture of risk awareness among individuals as well as at the overall institutional level. Operational risks frequently appear in places where they are the least expected, because generally "something like this" has "never happened before" and "especially not here." This is why relying solely on past experience does not seem to be a viable option in this context. In contrast to the other risk categories, for which the risk sources are intelligible and fairly clear, the challenge is to anticipate as many aspects of operational risk in a bank as possible, always bearing in mind Murphy's Law: anything that can go wrong will go wrong at some point. Thus, the only way to prevent or, at least, limit damages that may occur is to develop the appropriate procedures.

Operational risk management is doubtlessly a type of risk management different from others because it is not limited in its scope to a division of a company or a line of business; moreover, the nature of the various sources of failure – processes, people, systems – varies widely and requires a broad range of preventive and control mechanisms. On the assumption of a uniform definition of operational risk that makes reference to the source and is preferably oriented on the Basel definition, operational risk management concerns the entire bank. The different possible forms of operational risk must be identified and assessed as regards their potential for damage and the processes for preventing and limiting risk must be installed; the objective is to anchor a way of dealing with risk just as strongly in the corporate culture as the risk itself is linked to the nature of the business operations.

1 *See BCBS (2001), p. 13.*

The comprehensive nature of operational risk management makes it a task that cannot be tackled by a small team of specialists alone but also needs the support of senior management and the entire management staff. Indispensable in this context is continuous, open and direct communication in both directions, not only to properly capture and assess the risk situation, but also to achieve the necessary acceptance of the measures linked to the introduction of the framework.

However, simply implementing a risk management framework at one time is not enough because sources of risk change over time. Therefore, it must be part of the new risk culture to create and maintain a proactive system that ensures the ongoing adjustment to any changes. Apart from the establishment of new processes to assess operational risks that may arise from new products, distribution channels or lines of business, what is also necessary is the setting up of a workable reporting system to communicate existing weak spots and the need to make changes to the framework in the future and to enable a response to cases of damages not by pointing fingers but by preparing concrete countermeasures.

The last highly topical aspect of operational risk management concerns the implementation of the Basel II provisions. The numerous parallel projects underway for the purpose of implementing the new rules will have far-reaching impacts on banks' activities at the organizational and technical levels. Workflows need to be restructured, systems need to be enlarged and maybe even new ones created. It is an enormous task that carries the risk of having a dynamic effect on operational risk because the complexity of the projects creates a certain susceptibility to error. New, unfamiliar processes may carry a higher risk potential in the initial phase of adjustment, just as newly developed IT systems are potential sources of error. Thus it may very well be that the implementation of Basel II, which had been set up to control and mitigate risks, could in fact increase operational risk. This heightened risk would not be discernible at all at the level of the formal calculation of capital charges with the less risk-sensitive approaches (BIA, STA); the more sophisticated approaches (AMAs) and their models based on historic loss data would discover the risk only with difficulty or (too) late. The only way to recognize and avoid this risk is by consistently conducting assessments of the risk situation and maintaining a functioning system of quality assurance during the implementation of an operational risk management framework. This includes quality control measures for project work and software development as well as sufficient training for the staff affected by the changes.

Conclusions

Ultimately, there is no way around operational risk management at banks – either by implementing the framework proposed by the Basel Committee on Banking Supervision o a slightly adapted version. This has little to do with whether or not Basel II will be introduced as scheduled; rather, in many areas there is an unavoidable need to bring management methods up to date with the risks that actually exist at present, among which there are a few that have been underestimated or even overlooked up to now. Operational risk management is not a futile exercise and cannot be regarded as a real additional burden.

Many of the measures foreseen would have to be implemented sooner or later for reasons of prudence, even without Basel II; and in fact, some banks have already taken these measures before and, especially, during the discussion about the Basel Accord.

Nonetheless, the positive side effects of implementing an operational risk management framework are frequently disregarded even though the creation of higher risk awareness and transparency, the improvement of process quality and the significant reduction in the number of cases of damages or loss by applying operational risk management is doubtlessly valuable in itself and constitutes a vital contribution to overall banking management. Successful risk control and mitigation by maintaining an effective operational risk management framework will without doubt enhance a bank's profile, and ultimately also give it competitive advantage because one thing is clear: regardless of who – passenger or crew member – no one likes to find themselves in distress at sea.

References

BCBS – Basel Committee on Banking Supervision. 1998a. Framework for Internal Control Systems in Banking Organisations. Basel Committee Publication 40. Basel: Bank for International Settlements. October 28, 2003: http://www.bis.org/publ/bcbs40.pdf

BCBS. 1998b. Operational Risk Management. Basel Committee Publication 42. Basel: Bank for International Settlements. October 28, 2003: http://www.bis.org/publ/bcbs42.pdf

BCBS. 1999. A New Capital Adequacy Framework. Basel Committee Publication 50. Basel: Bank for International Settlements. October 28, 2003: http://www.bis.org/publ/bcbs50.pdf

BCBS. 2001. Working Paper on the Regulatory Treatment of Operational Risk. Working Paper 8. Basel: Bank for International Settlements. October 28, 2003: http://www.bis.org/publ/bcbs_wp8.pdf

BCBS. 2003. Sound Practices for the Management and Supervision of Operational Risk. Basel Committee Publication 96. Basel: Bank for International Settlements. October 28, 2003: http://www.bis.org/publ/bcbs96.pdf

BIS – Bank for International Settlements. 2001. The New Basel Capital Accord. Consultative Document. January 2001. Basel: Bank for International Settlements. October 28, 2003: http://www.bis.org/publ/bcbsca03.pdf

BIS. 2003. The New Basel Capital Accord. Consultative Document. April 2003. Basel: Bank for International Settlements. October 28, 2003: http://www.bis.org/bcbs/cp3full.pdf

Brandner, A., B. Bruckner, C. Kanneberger and K. Royer. 2002. Operationelles Risiko in Finanzdienstleistungsunternehmen – Fallbeispiele aus den Bereichen Asset-Management und Security Trading. In: Eller, R., W. Gruber and M. Reif (Eds.). Handbuch Operative Risiken. Stuttgart: Verlag Schäffer- Poeschel.

van den Brink, G. 2001. Operational Risk – Wie Banken das Betriebsrisiko beherrschen. Stuttgart: Verlag Schäffer-Poeschel.

Utz, E. R. 2002. Bedeutung Operationeller Risiken aus Sicht von Banken und Sparkassen. In: Eller, R., W. Gruber and M. Reif (Eds.). Handbuch Operative Risiken. Stuttgart: Verlag Schäffer-Poeschel.

VÖB – Bundesverband Öffentlicher Banken Deutschlands. 2001. Aktuelles II/2001. October 28, 2003: http://www.voeb.de/content_frame/downloads/2_2001.pdf