



FINANCIAL SERVICES

Managing Operational Risk Beyond Basel II

ADVISORY

Contents

Introduction	1
The Current Environment: The Basel II Experience for Major Banks	2
Regulatory Influences	3
The Way Forward	3
The Components of Managing Operational Risk: Lessons Learned	4
Operational Risk Strategy	4
Organizational Structure	5
Reporting	5
Building Blocks	5
Information Technology	7
Looking Ahead	8
The Opportunity: Addressing the Gaps	9
Integrating Compliance and Performance	9
Improving Data Quality and Reporting	10
Evolving to Integrated Risk Management	10
An Approach to Aligning Operational Risk Management with Performance Management	11
Methodology to Supply Information for Decision Making	11
Integrating Operational Risk Information with Decision Making	12
Conclusion	13
Appendix I: Review of AMA Models – Recent Experience with Major Banks	14
Introduction	14
KPMG’s Project Approach for AMA Reviews	14
Summary of Findings	15
Conclusion	16
Appendix II: Enhancing a Bank’s Insurance Portfolio	17

Introduction



Many banks have invested significantly in improving their operational risk management in the last few years to comply with Basel II. Specifically, banks have invested in:

Resources. Increasing support resources, investing in knowledge building, and creating awareness through training.

Processes. Developing and implementing methodologies to assess, monitor, manage, and model their operational risks.

Technologies. Implementing solutions and tools to assess, monitor, manage, and model their operational risks.

Most of the effort has focused on compliance with Basel II and other regulatory requirements, and some banks continue to struggle with this process as they work through the approval process. Leading banks, however, have risk management frameworks in place and are now seeking to make the process significantly more relevant to management decision making.

These banks are now considering the value of these efforts (specifically those associated with managing operational risk) and what returns they could derive from them. As a result, banks are evaluating how to build on lessons

learned from Basel II implementation, regulatory approval preparations, and regulators' feedback. An emerging goal is to leverage their investments in operational risk management to make better decisions and enhance business performance.

To derive business value, banks must integrate their operational risk management into their strategic and day-to-day business decisions. By understanding their risk and control environment better, for example, banks should be able to reengineer their business processes to be more effective and efficient. However, linking operational risk management to performance management is easier said than done. It involves a change of organizational mindset as well as a defined means of aligning the management of operational risk with business performance.

This white paper explores these issues. It reviews the components of the operational risk management process in place at many banks. It considers the lessons learned from the operational risk management investments that have been made, the opportunities that have resulted, and experience gained from the regulatory approval process. This paper proposes an approach to aligning operational risk management with performance management.

Jörg Hashagen

Global Head Advisory Financial Services

The Current Environment: The Basel II Experience for Major Banks



Figure 1: Framework for Managing Operational Risk



Source: KPMG International, 2005

Market experience with achieving the standard required for Basel II compliance over the past three years has resulted in a number of lessons learned. Perhaps the most significant of these lessons are those related to calculating regulatory capital for operational risk, especially for the major banks in Europe and Australia that chose to apply for the Advanced Measurement Approach (AMA). Implementing the Basic Indicator Approach (BIA) or the Standardized Approach (TSA) provided useful insights for all banks, not just those aiming to move to more sophisticated approaches later.

Many banks are now managing operational risk much like credit or market risk, using formal frameworks such as that depicted in Figure 1.



Among the most advanced efforts for AMA banks has been to develop and implement robust governance structures (encompassing risk strategy, organizational structure, and reporting) making operational risk a formal risk category requiring ongoing management.

These efforts have resulted in improved infrastructure such as the development of operational risk management committees at both the entity and business levels and the increased (and more formal) consideration of risk in change management and project initiatives. This focus on operational risk, now present in many banks' governance structures on a par with other risk categories, has elevated the importance of operational risk and its influence across the organization.

BIA and TSA banks can use the same framework and blocks as AMA banks but usually spend less effort in some areas (especially modeling), a focus that is understandable and appropriate. At the same time, they may not have concentrated on other areas, such as data collection and management structure, and this lack of focus could be detrimental over time.

Regulatory Influences

Regulators' approaches to Basel II—specifically, the degree of detailed guidance and interpretation they provide—differs widely across regions. Although regulators have had considerable influence on banks' efforts to manage operational risk, the variation in their approaches means that achieving a level playing field will not likely be realized in the short term.

In some jurisdictions, for example, regulators have been heavily focused on governance structures—areas such as how the organization demonstrates independence, its use of appropriate processes, and whether the right information is being communicated. In other jurisdictions, regulators use these structures (and the information flowing from them in reports, minutes, and actions) as evidence of a functioning risk management system.

In other areas, leading organizations are defining the expectations rather than depending on the regulator to do so. For example, in considering the components of operational risk modeling driven by Basel II—e.g., internal loss data (ILD), external loss data (ELD), scenario analysis, and the business environment and internal control factors—many regulators have given the greatest weight to ILD because of the ability to reconcile “real” data to the general ledger. Although ILD is a tangible, measurable statistic, many banks have come to recognize its

weakness as a valuable input to the holistic risk process—simply because historic losses may not be a valuable predictor of future trends. This issue arises more frequently in Europe—where regulators tend to prescribe the components of models—than it does in Australia, for example, where the focus of operational risk management has shifted toward scenario analysis. The bottom line: around the world, banks set limits, but regulators influence the focus of their attention, and that focus varies by jurisdiction.

The Way Forward

As Basel II compliance continues to evolve, the process has resulted for many banks in a number of lessons learned from which many others can potentially benefit. The next section of this paper discusses the components of an operational risk framework and some aspects of banks' experience in applying such a framework.

The Components of Managing Operational Risk: Lessons Learned



The experiences of several major banks that have developed and implemented methods and processes for operational risk management over the past 10 years point to better practices and ideas. The discussion below describes the components of operational risk management along with some lessons learned by many banks in addressing these areas.

Operational risk occurs throughout organizational units, and it encompasses a wide range of loss scenarios—from small losses resulting, for example, from errors in order management to large losses resulting from fraudulent actions. Moreover, operational risk losses often cannot be separated clearly from those resulting from credit, market, or other risk types. Consequently, the measurement and management processes for operational risk can deviate significantly from the processes associated with managing other risk types.

The process for managing operational risk encompasses:

- Identification of key operational risks
- Qualitative and/or quantitative

- assessment of the identified risks
- Reporting of the results of the identification and assessment
- Management in its narrow sense (i.e., taking measures to mitigate risk)
- Monitoring of the effectiveness and efficiency of the measures.

A framework for managing operational risks is shown in Figure 1 on page 2. Such a framework can vary in size and complexity, timing of implementation, and level of sophistication, but in some form is common among banks either ready or getting ready for Basel II. Because of their nature, such frameworks also remain relevant in contexts beyond regulatory compliance, but their focus may have to evolve to better support management. The components of this framework are briefly described below.

Operational Risk Strategy

The definition and adoption of a risk strategy is a central element of Basel II's Pillar 2. The risk strategy should encompass all the relevant risk types. It should be aligned with the business strategy and should be adjusted periodically by those at the

highest management level to reflect recent developments in the business. It can be a stand-alone operational risk strategy or a component of an overall organizational risk management strategy.

The operational risk strategy typically encompasses the following areas:

- An operational risk definition and an identification of sources for operational risk
- A description of the specific risk profile (for example, the main risk drivers depending on size and complexity of the business)
- A definition of the objectives—in particular the organization's appetite for operational risk—expressed in a measure useable for management purposes
- A high-level description of the instruments used for operational risk management
- A description of the responsibilities and of the integration of operational risk management into overall risk management at the bank-wide level.

Lesson Learned

Establish realistic objectives and gain board support.

Perhaps the most important prerequisite for successful operational risk management is to establish realistic objectives that have clear economic benefits and the full support of the board and senior management. Some banks' early experience showed that efforts that did not sufficiently support strategic and tactical management could not gain the support of senior management and thus were not readily accepted at other levels.

Organizational Structure

Adopting an organizational structure is an important step in the process of managing operational risk. Figure 2 depicts a generic organizational model.

Managing or transferring operational risks largely depends on the size and complexity of the organization's activities and products. The importance of this effort, and the prevalence of operational risk across the organization, means that its implementation should be carried out by an entity-wide risk management committee reporting to

the board. As with the management of other risk types, such an operational risk management function would be responsible for developing operational risk management instruments for the entire organization, with the support of decentralized risk management staff.

Lesson Learned

Define responsibilities across the organization.

A common misunderstanding is that a central unit (the operational risk management function) may become responsible for the actual management and mitigation of operational risks. In fact, the operational risk management function should be responsible only for coordinating and supporting the activities of the individual business areas and support units, which are, in turn, responsible for actual risk management. Defining responsibilities and obligations to cooperate and communicating this information—in particular compared with efforts of established units such as Internal Audit, Quality Management, IT-Security, BCM, and others—are critical to the success of the effort.

Reporting

Operational risk reporting is an essential part of risk management and monitoring by the board and other decision makers. Reporting should be a routine and standardized process, ideally carried out by an independent party, usually the operational risk management function. The risk report may be focused solely on operational risks or cover all risk types. For operational risk it is particularly important that results from quantitative and qualitative risk assessments are consolidated and reported in a homogeneous framework.

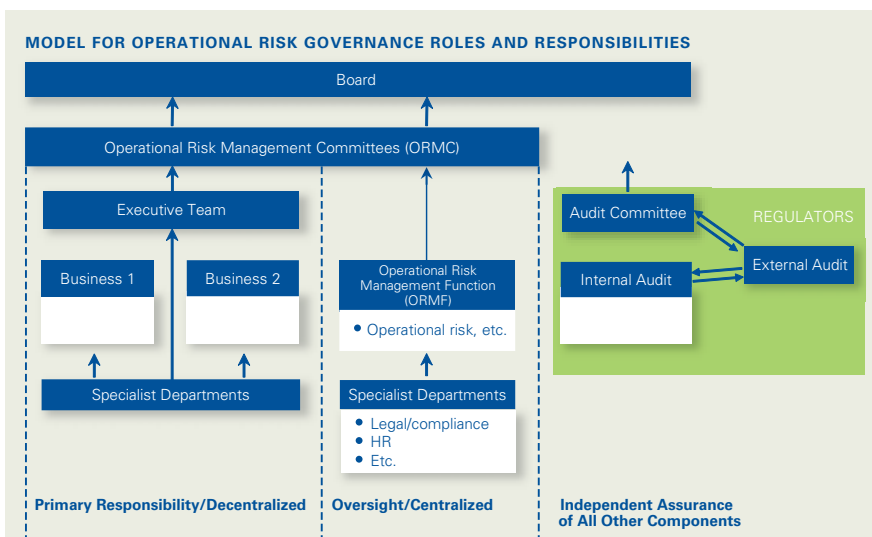
Scope, content, timing, and recipients of the reporting depends on the organization's specific risk profile and the selected operational risk strategy. The board and other decision makers—such as the operational risk management committee, if in place—should be regularly briefed about major loss events and significant operational risks as well as receive briefings on an as-needed basis.

Lesson Learned

Ensure reporting will add value.

Effective collection of risk information for reporting depends on appropriately established and communicated incentives. Without the support of qualified people across all business units, data collection will likely be incomplete and, worse, reports may lack relevance and added value for decision makers, who may then ignore or even actively oppose them. The organization should carefully consider at an early stage the requests and requirements of those who will ultimately use reported information.

Figure 2: A Model for Managing Operational Risks



Source: KPMG International, 2005

Building Blocks

Definitions, Linkages, and Structures

To manage the wide spectrum of operational risks, the organization should define risk sub-categories. These sub-categories could be, for example, oriented toward the common definition and thus could classify operational risk causes into processes, people, technology, and external influences.

Loss Data

The systematic collection of information about operational risk losses is an essential basis for developing quantification methods. Loss data are also used for validation of both quantitative and qualitative risk assessments as well as for early-warning risk systems. Loss data are key to identifying risk causes, to deriving risk management measures, and to reviewing the effectiveness of such measures realized beforehand.

Lesson Learned

Establish structured collection of internal loss data.

Set specific incentives for loss data collection, establish transparency at all organizational levels, and establish a sanction process for cases of non-compliance. Even with such measures in place, organizations can expect to spend one to three years until a new process for loss data collection provides high-quality results.

Losses can be structured by cause, event, and effect. In addition to losses that occurred directly, the organization can capture indirect losses (including, for example, follow-up costs as a result of overtime or foregone revenue) and near misses (such as events where actual losses are prevented at the last minute). The organization should collect all loss data above a de minimus threshold at regular intervals.

Core information from loss data includes:

- Gross loss amount (that is, before any recovery)
- Insurance benefits and other recoveries
- Respective risk category
- Business area where the loss occurred
- Date of occurrence and date of discovery of the event
- Business area primarily responsible for the risk management of the loss (usually the business area in which the damage was caused)
- Cause(s) of the event.

The operational risk management function should set up a process to collect valid loss data. Severe losses are usually rare but their identification and

reporting are essential for identifying and preventing potential risks.

Therefore, internally collected loss data covers only the least severe part of the universe of all possible events. External experiences should also be considered and collected either from publicly available sources (through their own investigation or from commercial suppliers) or from participation data sharing ventures.

Risk Assessment

Qualitative risk assessment is usually a self-examination process. Typically, the operational risk management function conducts interviews among various employees (usually with the aid of questionnaires or workshops), focusing on their assessment of defined risks or risk areas. Concrete measures for risk mitigation are derived from the results.

To maintain objectivity, an independent unit (such as the organization's operational risk management function or internal audit group) would conduct the risk review and evaluation. The organization should conduct such a self-assessment at least once a year, determining appropriate time intervals based on its risk profile, changes in risk areas, and other external factors.

The self-assessment encompasses a quantitative assessment of the potential for various risks based on existing risk mitigation measures. (The organization can also conduct a gross evalua-

tion without consideration of existing measures.) Risk exposure is often determined by separate estimation of the particular risk's probability of occurrence (likelihood) and the amount of loss that could result (impact). The result can be represented in a matrix format; see Figure 3. The bubbles in the matrix could, for example, represent business units or event types.

Lesson Learned

Conduct regular structured risk self-assessments.

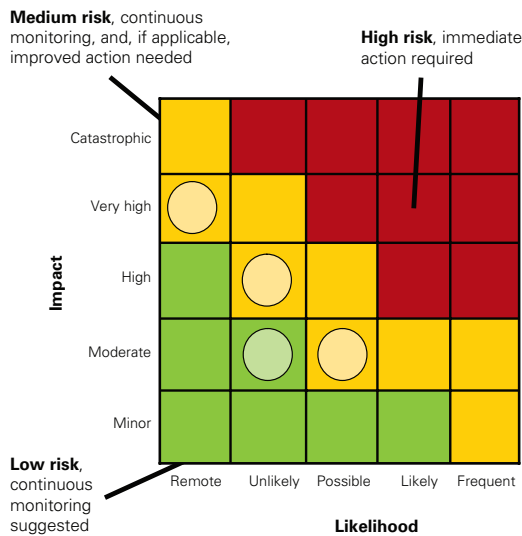
Like loss data collection, self-assessment efforts suffer from start-up-difficulties. Organizations must take steps to counter the human inclination to underestimate the severity and frequency of risks. Results of high quality are often attained after repeated self-assessments. However, too frequent or too standardized an assessment can lack value.

Key Risk Indicators

One major aspect of operational risk management is the early identification of changes in risk potential that could lead to future losses, with the goal of preventing those with the highest probability. Methods are frequently based on key risk indicators (KRIs)—including, for example, cancellation rate, sickness ratio, or failure rate—which can be both quantitative and qualitative in nature.



Figure 3: Estimation of Loss Potential as a Basis for Qualitative Methods



Source: KPMG in Germany, 2007

The focus on prevention is important for selecting and defining KRIs and for determining thresholds. The frequency of collection has to be compatible with the nature of risk mitigation measures, which are comparatively short-term in relation to self-assessment.

Lesson Learned

Consider the value of KRIs.

Many AMA banks experience ongoing difficulties with developing and deploying useful KRIs. Industry leaders largely agree that organizations should have the ability to directly correlate specific measures with the likelihood of increasing risk exposure. In reality, however, lack of readily available useful information means that the potential benefit from such indicators may not outweigh the cost and effort required at the business-unit level to develop and implement them.

Mitigation

Mitigating operational risks focuses on establishing a balance between the target defined in the risk strategy and the current state. Reporting is used as a starting point for deriving measures. Causes for significant losses (for isolated cases or cumulatively) are specifically analyzed.

Fundamental alternatives for decision making are:

- Conscious acceptance of existing risks
- Risk transfer to a third party (e.g., through insurance)
- Risk avoidance by means of closing business activities
- Risk mitigation by means of other risk management measures (such as employee training, extension of control systems, and introduction of IT system for automatic fault identification).

These measures are supplemented by business continuity management frameworks, which aim to limit losses and facilitate prompt resumption of business operations in the event a catastrophic risk cannot be prevented.

Lesson Learned

Coordinate all appropriate resources to mitigate risk.

As operational risk mitigation is partly a central and partly a local responsibility, coordinating the mitigation activities to avoid gaps and redundancies is important. Furthermore, in certain situations (such as with BCM programs), bringing together specialized knowledge (e.g., from the IT department), business knowledge, and risk information can also be useful.

Capital Modeling

Quantitative assessment of operational risk requires measurement models. Such models are often based on simple estimation methods; few companies use an explicit quantification approach for operational risk—a sign that appropriate models for operational risk are still evolving.

Nonetheless, operational risks can be modeled using methods from actuarial risk modeling, such as the collective model or Extreme Value Theory (EVT). The majority of these bottom-up approaches are based on historical loss data or on estimation of potential loss scenarios. EVT can be used for explicit consideration of severe and rare losses. The result of the quantification is usually an expected loss (which should be entered into the product calculation as a component of standard risk costs) and an unexpected loss (difference between percentile and expected loss), which should be integrated into the company's economic capital together with the values of the remaining risk types.

Lesson Learned

Base quantification methods on a mature operational risk framework.

Operational risk quantification requires that appropriate data are available of high quality and with adequate history—so that the results can have value. Preconditions must be established so the results reflect organizational management efforts. Starting the quantification without creating an appropriate foundation for it—one embedded in the risk strategy—overestimates the importance (and capabilities) of the method and its results. Data quality is critical.

Information Technology

The IT infrastructure needed to support the process of operational risk management can range from simple data-entry forms for the collection of loss data and the performance of risk assessments to specialized, integrated, Web-based applications and databases.

Basic functions of integrated software packages for operational risk are:

- Decentralized data entry (loss data, risk indicators, replies to risk-assessment questionnaires)
- Decentralized ad hoc evaluation in the various business lines (for example, evaluation of loss-data histories, computation of business-line-specific indicator scores, determination of a risk-assessment rating)
- Centralized evaluation across all business lines (determination of regulatory and economic capital; aggregation and comparative presentation of the results of all components of operational risk for board reporting purposes)
- Centralized and/or decentralized administration (user data and other static data).

Lesson Learned

Depend on IT as a tool—not a problem solver.

Specific software for operational risk can help with the execution of an already defined and established process. However, without establishing an organizational structure, specifying the methods to be applied, and clearly defining their processes, the introduction of an IT tool is useless at best and harmful at worst. The allocation of both financial and human resources must be in line with activities that support risk management if the tool used is to be effective.

Looking Ahead

The risk and finance functions in many banks are now balancing their efforts to influence strategic direction. Pillars 1 and 2 are bringing the finance and risk communities closer together as well as aligning their focus on performance management, with risk as a driver and



capital as the ultimate lever. This advance should enable an organization to demonstrate a comprehensive understanding of risk in the context of the organization's strategic objectives and tactical targets.

The regulators welcome these developments. They want the operational risk models to be sound, but they are putting equal emphasis on how operational risk management is embedded in the business—specifically, whether the decision-making processes are working, whether the models are supporting those processes, and that the results are used. Thus, when applied in more than just a regulatory context, Basel II is adding real value. As a result of increased focus, operational risk management is becoming a more important function in the business.

What's more, operational risk information is improving: Operational risk was largely irrelevant five years ago, because the available information was considered inaccurate, too technical, or otherwise lacking business value. Increasingly useful information is finding its way into the management structures of the organization, and as the information improves, it cannot be ignored.

The next section considers the business improvement opportunities banks now have in the wake of compliance.

The Opportunity: Addressing the Gaps



Although Basel II was developed to help banks improve risk management, it quickly became perceived by many banks as yet another regulatory compliance obligation. Meeting its requirements was initially so complex that, like Sarbanes-Oxley, Basel II seemed to create more work than value. For most banks—facing time and resource constraints and under pressure to gather extensive information and meet compliance deadlines—the focus became meeting the requirements rather than driving business value from the effort.

In addition, compared with credit risk management (the more mature process, but one that also required a major effort to reach Basel II compliance), operational risk management suffered from either an inaccurate perception about its nature or a lack of appropriate understanding by senior management—many of whom believed they were already managing these risks. Operational risk management has also been affected by a lack of resources, little regulatory guidance on specific but key issues, and few proven methodologies, processes, and tools.

Now, however, with several years of Basel II implementation experience behind them, banks have a new opportunity to integrate operational risk management into day-to-day and strategic decision making to provide value to business and management. Specifically, they can now:

- Identify the “gaps” between being Basel II compliant and managing business performance. (These gaps are independent of the approach taken by the bank—i.e., BIA, TSA, or AMA—but are in most cases larger for BIA and TSA banks than for AMA banks, primarily due to the extent of the compliance effort needed.)
- Seek to understand the benefits of addressing these gaps as opportunities to improve performance while simultaneously reducing operational risk.

Achieving these results calls for a number of key steps, as discussed in the remainder of this section.

Integrating Compliance and Performance

Many of the traditional operational risk management areas—including IT security, compliance, legal, or insurance—continue to work in silos rather than in an integrated manner. Their efforts tend not to be fully coordinated with the operational risk management function or supervised by a risk or an operational risk management committee.

In many cases, these individual operational risk management areas use their own instruments for risk assessment (e.g., independent assessment for business continuity or anti-money laundering, independent set of indicators to measure IT-security risk, and so forth) or use similar ones, but not in a consistent manner, which creates considerable potential for overlap. These areas may work completely independently and are not integrated with operational risk management.

Indeed, most banks have not integrated into day-to-day management the instruments for identification and measurement of operational risk (efforts that are required for the AMA).

They use these instruments for regulatory purposes—specifically, to calculate regulatory capital or as a means of notifying the operational risk management function of important issues. Moreover, in most cases local operational risk management does not use its own operational risk data to influence local business decisions. Potential reasons may be:

- Limited real or perceived relevance of data for day-to-day management
- Limited understanding of operational risk data and outcome
- Limited access to the data or use of the existing unconnected instruments for more detailed analysis.

Consequently, in many banks, the operational risk management function neither supports the strategic and day-to-day decision-making process of the bank nor provides substantial management information to business lines. It may conduct an after-the-fact analysis of business decisions—such as those involving outsourcing, penetration of new markets, or launch of products and services—but its work is not integrated into the strategic planning efforts that drove those decisions. Having been set up for regulatory compliance in the first place, operational risk departments typically compile information of a type and in a manner that management does not find useful.

Improving Data Quality and Reporting

Operational risk is often still seen as the outcome of negative effects, such as human failure, and the desire to disclose such information is understandably limited. Data quality (i.e., completeness, accuracy, and coverage) is slowly improving. However, sustainable data quality can be achieved only if local risk management accepts the data as the most important basis for their risk management activities and finds it in their own best interest to maintain it at a high level of quality. Senior management has a critical role in establishing clear incentives to ensure and enhance data quality.

Once the data is compiled, operational risk reporting usually flows in one direction only—from the business units

to the operational risk management function. An aggregated report is typically sent to senior management, but in most cases the business units do not receive consolidated reports based on their data and tied to their individual risk profiles. Often what the business units do receive may not be relevant to their needs, which reinforces the negative perception of the process and its output. Improving the flow of information would require a change in mindset (specifically, the willingness to rely on and use the data for more than regulatory purposes). The result, however, could be improved information transparency and better analytics that would improve the data's relevance to the business.

Evolving to Integrated Risk Management

The opportunity now for banks is to integrate operational risk into the local day-to-day business management (not only risk management) and make operational risk measurement and analysis a core element of strategic decision making. To do so, management must align and coordinate the different operational risk management activities within the bank and make results of individual risk analysis comparable between different areas.

Regulatory compliance tends to focus on risk capital and implementation of minimum standards in a cost-effective manner. However, better practice risk management ensures that operational risk is considered in any decision-making process. Specifically,

- A comprehensive view on the risk profile of all areas of the bank enables much more informed decision making
- Coordination of risk management activities prevents overlap and inefficiencies, thereby allowing management to leverage resources available for risk-reducing measures (e.g., insurance programs, business continuity management)
- Including risk analysis of new products, processes, systems, or markets in business decision making helps management decide on countermeasures in an early stage of the decision-making process

- A deeper understanding of operational risk at the business-process level supports the enhancement of these processes or systems and can have a direct influence on improved performance

Principles of an Ideal "Future State"

Each bank's situation is different but a few principles of robust operational risk management hold true for leading institutions:

- Risk at the group and the business unit levels is defined and communicated. Business unit operational roles and responsibilities are clear, specific, understood, and applied with rigor. The risk management function "owns" the risk profile—it provides oversight and the business unit personnel are accountable for implementing the profile.
- The risk management function is recognized as providing independent oversight of the organization's risk profile.
- Risk management activities are focused on enhancing and generating business value. The risk function is actively sought out as a participant in the business development process. It is perceived as forward-looking, engaged in new initiatives, focused on strategic planning, and aware of what risks the organization can take.
- Risk is perceived holistically, and its definition includes all the elements that constitute the real risk of achieving an expected return within the guidelines of the organization's risk appetite.
- Risk is measured as accurately and as frequently as possible, from the top down (strategically) and from the ground up (tactically).
- KRIs enable the constant monitoring of the evolution of the risk profile (KRIs will be a work in progress for some years to come).

The next section considers an approach to achieving these goals.

An Approach to Aligning Operational Risk Management with Performance Management

Basel II has prompted banks to gather operational risk information for compliance purposes. Now that compliance efforts are established—or, for those still in the midst of the process, a clear path is visible—the challenge is to derive new business value from operational risk information and related processes—specifically by aligning the management of operational risks with efforts to improve business performance.

Organizations can benefit from a process that helps them link the operational risk framework more closely to the risk reporting, management, and monitoring efforts that are key aspects of enhancing business performance (see Figure 4).

This endeavor starts with efforts to identify and assess operational risk information to improve business and risk management decision making. The focus should be on identifying the risk information decision-makers need to improve the cost-benefit analysis of business opportunities.

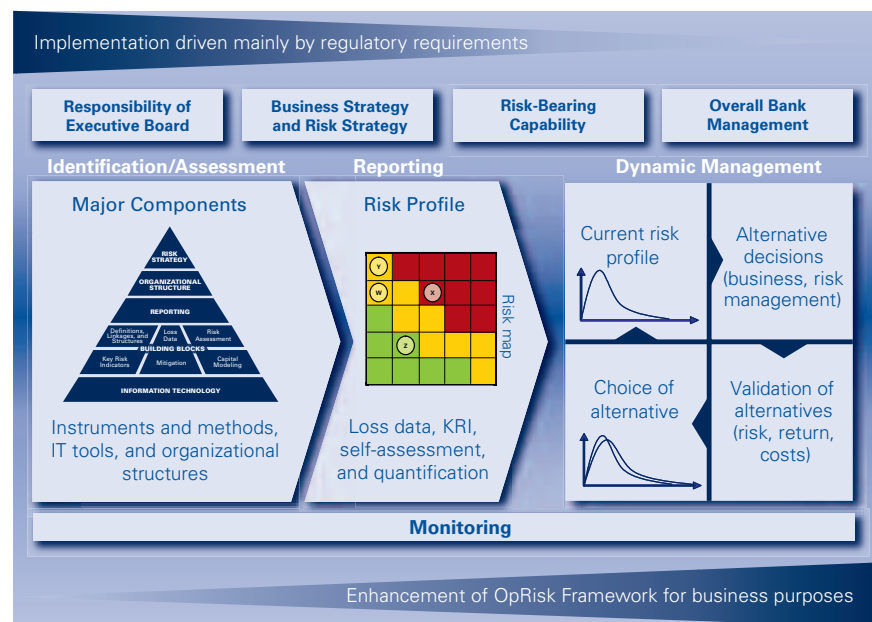
Methodology to Supply Information for Decision Making

Operational risk information can support a variety of decision making, as discussed below.

Business Decisions

Operational risk information better enables strategic business decisions (such as those involving investments, M&A activities, expansion or contraction of business areas, and outsourcing) as well as day-to-day business decisions (involving, for example, efforts to enhance processes or skill sets).

Figure 4: Aligning Compliance with Performance



Source: KPMG in Germany, 2007

Current efforts to manage operational risks typically take place after business decisions have been made. Ideally, however, knowledge of these risks, and efforts to manage them, should become part of the decision-making process. When considered early in the process, operational risk information can help decision makers evaluate the risks inherent in various choices, develop risk/reward calculations, and determine how subsequent alternatives would affect the organization's risk profile.

The methodology in place at most banks, however, is not sufficiently robust to support this kind of analysis. Indeed, in the bigger picture, culture and tradition typically have greater influence over decision making than methodology and data availability. In addition, many banks' business is still volume driven; better decision making

will evolve with a shift in focus from pure volume to an equation in which decision makers balance risk and reward information.

Improving the Process

Operational risk management methodologies and processes can be used in a number of ways to enhance business decision making. For example:

- **Scenario analysis** can help organizations find the optimal balance between risk appetite and cost reductions. Decision makers can use scenario analysis strategically—ideally in conjunction with an estimate of the influence on value-at-risk (VaR) in an economic capital setting—to judge risk-adjusted profitability and thereby forecast the influence of strategic decisions on the organization's operational risk profile.

- **Economic capital calculations** enable organizations to use operational risk information to evaluate the risk-adjusted returns on potential investments or new businesses.
- **Process efficiency** efforts should be aligned, to the extent possible, with operational risk management to achieve the best result in each area. Enhancing processes can lead to a reduction of operational risk as the process structure becomes increasingly transparent and better documented. However, when controls are eliminated or staff or IT capacities are reduced to cut costs, operational risk might increase.
- **New-product approval processes** are enhanced when they encompass operational risk management. In the past, risk management in this area has often meant simply checking for signatures or other evidence of compliance. Instead, operational risk information should be considered in every aspect of new-product processes—such as marketing, sales, back-office, accounting, legal, training, and IT—so decision makers can analyze what risks are inherent in the new product and provide their judgment on that product and the risks it may pose to the organization.

Risk Management Decisions

Operational risk information is also useful to derive decisions aiming primarily at adjusting the risk profile. Such decisions can involve the strategic (e.g., insurance portfolio enhancement, business continuity management, capital management planning, and alternative risk transfer) or the day-to-day risk management (e.g., enhancement of controls, introduction of new products). The important step is to establish a regular flow of information between the operational risk management function and functions including IT, legal, insurance, or the purchasing department. Such communication can help organizations make sure their decisions include an overall view of risk (and are not based solely on one factor such as price).

Integrating Operational Risk Information with Decision Making

Improving the use of operational risk information calls for making changes in how the organization manages its operational risks—so that it can ultimately align this process with performance management. Addressing each aspect of the risk framework (depicted in Figure 1) can help facilitate the process, as discussed below.

In each of the framework areas, leaders should consider the following:

- **Operational Risk Strategy.** Take steps to ensure the operational risk strategy is aligned with the business strategy, and that updates are made continuously. Embed operational risk information into the business strategy development process to help improve overall performance outcomes.
- **Organizational Structure.** Intensify communication between the various business and support functions and the operational risk management function to facilitate increasingly informed decisions. Make operational risk management an integral part of decision processes. Establish committees to discuss cross-unit issues on a regular basis. Use this framework more efficiently.
- **Reporting.** Align the reporting contents, frequency, and recipients with decision-making needs. Improve the quality of the information reported and the degree of analysis provided with it (e.g., comparisons across time and units, benchmarking with external information, and so forth). Add value with information by considering what individuals need to know and how it can be supplied rather than what is available or what can be reported. Enable the operational risk managers to learn and use the business language so they can interact more effectively with business managers.
- **Building Blocks.** (Methods for identification and assessment). Make the information generated more reliable (i.e., more robust VaR models, quality assurance of self-assessments, and scenario analysis) and tailor it to enable ad hoc analysis in addition to scheduled calculations and assessments. Involve the business closely to increase relevancy of generated information and buy-in to the results. Aim to provide what is needed and continuously improve its quality and reliability.

These efforts could encompass the following adjustments to the methodology:

- *Definitions, Linkages, and Structures.* Align risk categories closely with the business needs rather than following regulatory standards with excessive strictness; keep the business unit and/or process structure up to date.
- *Loss Data.* Validate internal loss data with appropriate sources (such as the general ledger, claims handling, error reports) and avoid double work in collecting the data.
- *Risk Assessment.* Take into account not only the current controls structure but also expected changes to the business and the corresponding controls.
- *Key Risk Indicators.* Leverage existing MIS (e.g., on key performance indicators), use KRIs that management believes in rather than dictating KRIs from a central operational risk management perspective.
- *Capital Modeling.* Enhance the capital model to incorporate “what-if?” analysis on changes to the business, such as in the case of strategic decisions.
- **IT systems.** Help ensure IT can support decision making by upgrading operational risk systems to provide needed information. Make the system work for the business rather than allowing it to determine what information is gathered and reported.

Conclusion



As operational risk management efforts mature and gain both the support and the confidence of management, they are becoming increasingly valuable to the business. Conceived initially to support regulatory requirements, these efforts can be leveraged and aligned with business performance management.

To be successful, however, such alignment must be based on a clear vision of the potential benefits, with the risk team openly communicating what works and what does not in an implementation plan oriented toward management needs rather than regulatory deadlines. Some banks are at an earlier stage in the process, whether because of delayed regulatory deadlines or because they are endeavoring

to benefit from working their way through the continuum of Basel approaches. They can benefit because they have the opportunity to “get it right” from the beginning—specifically by combining regulatory and business requirements at an earlier stage. A defined framework, and focus on specific areas, can support this alignment and help banks gain new value from Basel II investments.

Appendix I: Review of AMA Models: Recent Experience with Major Banks*

Introduction

With the Basel II deadline for AMA compliance approaching quickly, many banks are in the process of finally reviewing their AMA frameworks or are in the midst of the regulatory approval process. They are having some difficulties that are both individual and general in nature. Drawing on individual experience may be difficult, but some lessons can be learned from considering the general aspects.

The lack of prescription in the regulatory requirements has presented a difficulty for the regulators and for those conducting AMA reviews. While this principles-based approach has been deemed beneficial—in that it enables banks to build processes, methodologies, and models suited to their particular environment—judging the degree of compliance with the requirements has been difficult. The qualitative AMA requirements are fairly new, and insufficient time has elapsed to determine the extent to which they are applicable or how they should be interpreted to be in line with better practice.

KPMG’s Project Approach for AMA Reviews

AMA methodologies include not only a quantitative model for calculating VaR but also a set of largely qualitative organizational, procedural, and methodological components to support the operational risk management process. The design and implementation of those qualitative methodologies and processes is generally more cumbersome than the actual quantitative model. Nevertheless, the quantitative models are still subject to numerous challenges due to the early stage of their development.

Figure 5 outlines both the steps of the risk management process that are common to other risk types (e.g., market and credit risk) as well as those that are more specific to operational risk. Although the structure of a specific bank’s AMA framework might look different, it is generally possible to map it into the common structure outlined next.

A number of regulatory requirements can form the basis for review; the exact list of requirements depends on the specific situation of the bank (e.g., Basel bank or not, location in EU country or outside the EU, subsidiaries in specific countries). Typically, as a minimum, the following documents are relevant:

- Basel II “International Convergence of Capital Measurement and Capital Standards: A Revised Framework, Comprehensive Version,” November 2006
- EU Commission Directive 2006/49/EC of the European Parliament and of the Council of 14 June 2006 on the capital adequacy of investment firms and credit institutions (recast), June 2006
- CEBS GL 10, Guidelines on the implementation, validation and assessment of Advanced Measurement (AMA) and Internal Ratings Based (IRB) Approaches, April 2006
- Any relevant local implementation of Basel II and/or the Capital Requirements Directive (CRD)
- Any relevant guidance from local regulators regarding the approval process.

Figure 5: Overview of Components of the Operational Risk Management Process



To provide a common structure to apply the contents of the documents listed above, organizations can use a matrix that enables structured consideration of the individual requirements (see Figure 6 for a schematic example). The matrix comprises the operational risk management process and its methodological components as depicted in Figure 5 on one axis and five corresponding categories to

Source: KPMG International, 2005

* First published in KPMG’s *Basel Briefing 12* and, in a modified version, in *OpRisk & Compliance*, July 2007.

analyze them on the other axis. These five categories are:

- **Qualitative and quantitative standards.** The specific requirements to be met by the process and methodology, such as data fields used, data history, calculation techniques
- **Validation.** The processes implemented in the bank to help ensure completeness and consistency of data and the application of methodologies
- **Documentation.** The extent, quality, and consistency in the description of the methodologies and processes
- **Governance.** The processes that help ensure appropriate ownership, control, and segregation of duties (e.g., between model development and approval)
- **Review.** The processes for continuous improvement to the methodologies and processes over time.

By coloring the matrix (e.g., using traffic light symbols), the operational risk manager can obtain a quick overview of the bank's state of preparedness to implement the relevant AMA approval process and identify necessary improvements.

A typical AMA review project offered by KPMG firms follow the time-based structure outlined in Figure 7. The time needed to complete such a project depends on the complexity of the methodologies and processes and the degree of preparation for the review.

Summary of Findings

Although the reviews at various companies differ in their results, the following issues occur frequently.

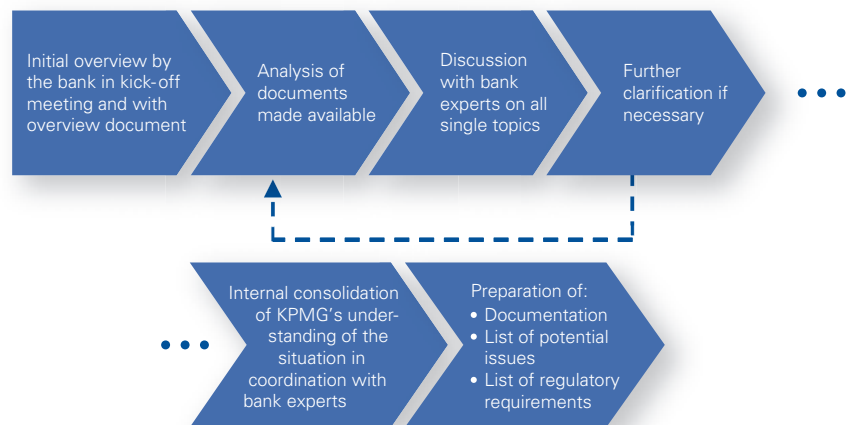
Documentation. A recurring theme in virtually all AMA reviews conducted is the quality of documentation. Documents are frequently not updated to reflect model or methodology developments, and inconsistencies are common among different documents. This problem is often due to the multi-year development effort that has taken place, where challenges have emerged and changes to the methodology have

Figure 6: Example Regulatory Requirements Matrix

	Qualitative and Quantitative Standards	Validation	Documentation	Governance	Review
Identification					
Internal Loss Data					
External Data					
Scenario Analysis					
Self-Assessment					
Key Risk Indicators					
Assessment					
Model					
Risk Assessment					
Reporting					
Management					
Risk Mitigation					
Monitoring					
IT Systems					

Source: KPMG in Germany, 2007

Figure 7: Project Approach for KPMG Firms' AMA Review



Source: KPMG in Germany, 2007

been required. This issue could pose a major threat to the application process: the bank's credibility can be damaged if inconsistencies emerge, or a lack of connection and cohesion is apparent, among various parts of the framework.

Use Test. A second key challenge is the required proof of use test. While the test result is usually demonstrated by integration of the operational risk framework results into the bank's governance structure, to be successful it requires the cooperation of all major business and support areas. This cooperation includes analysis of raw data and model results and basing subsequent management decisions on that analysis. At some banks, the integration of the operational risk management function with the business areas is not close enough to prove the use test concept in a simple way.

Model Governance. Another weak point in some banks is the model governance processes (e.g., manner of dealing with noncompliance, model change approval policies, and so forth). The focus of methodology and model development has often been handled on a project basis, with no real designed and implemented production processes (often called "business as usual") in place.

Data Quality. Data quality is also important, for both decision making and modeling purposes. Critical success factors include the accuracy and completeness of loss data, the validity of self-assessment, and scenario analysis results as well as the choice of suitable KRIs and their corresponding thresholds. Due to a lack of history of available data, comparing data either across time or across different instruments is often difficult.

Assumptions. Sound reasoning for all assumptions made in the AMA model is needed (e.g., the calibration of exogenous parameters) along with an appropriate description of the evolution of the models and their results. In a number of cases, banks have sound reasoning for the methodology components they have chosen but have not devoted enough effort to articulating why other components were not selected—a key requirement for many regulators.

Conclusion

AMA reviews can help banks prevent major surprises during the regulatory approval process. Experience built up through model and methodology reviews at other banks can support improvements for identified gaps in documentation and/or methodologies and processes before they are presented to the regulator.

Appendix II: Enhancing a Bank's Insurance Portfolio

Insurance products have always been one way of mitigating a bank's operational risk by transferring risk to the insurance market. In the past insurance was in many banks the responsibility of the procurement department. Moreover, decisions on insurance coverage were often based solely on the cost of insurance and the available budget rather than on a thorough analysis of the risk to be covered. Banks had somewhat limited knowledge of the insurance market—including factors such as available products, possible risk coverage, and capacity—which led as well to the fact that the aforesaid decision-making process was potentially influenced by external insurance brokers.

The use and importance of insurance management within banks is changing as operational risk measurement techniques continue to become more sophisticated. As a result of compliance with Basel II, banks' treatment of operational risk is now based on qualitative as well as quantitative information.

With decisions on insurance coverage dependent on the bank's risk profile, management of the insurance portfolio needs to be tightly linked with operational risk management. Although information from risk management is a fundamental basis for decisions on insurance requirements, the possibility of risk transfer should be compared with other alternatives. The decision on insuring a particular risk depends on:

- The type of risk and its wider impact for the bank on its short-term liquidity and reputation
- The level of risk appetite and the risk-bearing capacity of the bank
- The cost of risk versus the cost of risk mitigation
- The availability of insurance products and capacity

For AMA banks, the regulatory requirements for insurance play an additional, significant role in the decision process. The inclusion of insurance in the capital model, and any related reduction of operational risk capital, is subject to regulatory review and approval. This fact influences the decision on specific insurance coverage, the selection of the insurer, and the terms and conditions of the policy.

Apart from the qualitative criteria, the financial impact of the different options is of key importance in enhancing the insurance portfolio for both AMA and non-AMA banks. These factors could even be of higher magnitude than the potential relief on regulatory capital; thus, sometimes leading AMA banks to decide on insurance that does not comply with Basel II requirements. The financial components that must be considered include:

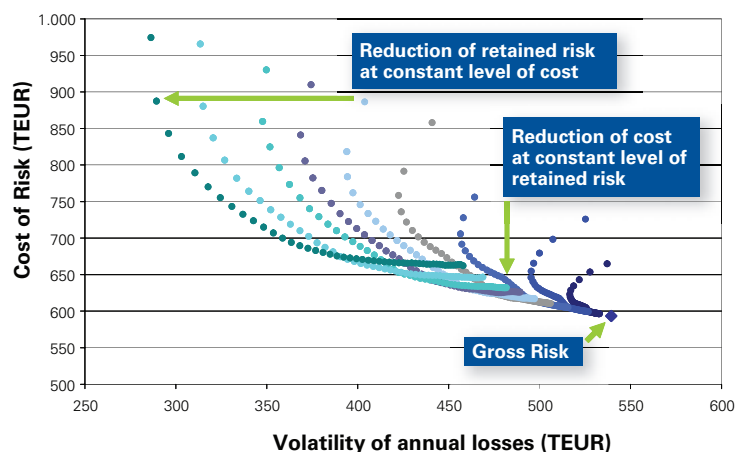
- Expected loss per annum as proxy for future realized losses
- Cost of capital (economic and/or regulatory) for retained operational risk (unexpected loss)
- Insurance premium
- Investments and cost of alternative risk-mitigating measures

In enhancing the insurance portfolio, the parameters of different policies need to be altered for an analysis of the effect on the risk profile. For example, the expenses for retaining risk, mitigation, and insurance coverage should be studied as a function of the deductible and payout limit of the insurance policies. Figure 8 below shows an example of the effect on the retained risk of changing the parameters of a single insurance policy.

The total costs (including capital cost, expected loss, and premium) are plotted as a function of the risk (in terms of volatility), each point in the graph representing a different set of insurance policy parameters with the identical underlying gross operational risk. By changing the policy parameters, different objectives of the insurance portfolio enhancement can be met. Either the retained risk is reduced while keeping the total cost at a constant level or the costs are reduced keeping the retained risk at a constant level.

AMA banks should calculate total cost and retained risk based on the same model used for capital calculation.

Figure 8: Influence of Insurance Policy Details on Retained Risk and Total Cost



When considering different operational risk types or business units, they could also utilize diversification effects within the bank for calculating the retained risk. Non-AMA banks could use a simple form (e.g., self-assessment, scenario analysis) for estimating their operational risk and expected loss.

The analysis and the enhancement can be extended from one policy to the insurance portfolio covering different risks. The effort for identifying the best portfolio structure and parameter combination rises with the number of policies. The enhancement process is thus focusing only on the most relevant insurances.

The parameters and the structure of the insurance portfolio can be balanced so that retained risk remains in line with the risk strategy established by the board of the bank. Enhancing the insurance portfolio allows risk managers to meet the board's risk appetite and its objectives for risk management while reducing the expenses on insurance coverage. The insurance portfolio analysis places the bank in a strong position to negotiate a policy's terms and conditions with the insurer. It also allows the bank to precisely state its requirements for insurance coverage and demonstrates a sound and professional operational risk management to the insurer—circumstances that could lead to a reduction of the insurance premium.



Contacts

Jörg Hashagen
Managing Partner Advisory
Global Head Advisory Financial Services
KPMG in Germany
+49 69 9587 2787
joerghashagen@kpmg.com

Marc Koehne
KPMG in Germany
+49 89 9282 1212
mkoehne@kpmg.com

Thomas Kaiser
KPMG in Germany
+49 69 9587 4114
thomaskaiser@kpmg.com

KPMG contributors to this publication include Thomas Kaiser, Marc Koehne, John Lee, Björn Lenzmann, Mike Ritchie, Diane Nardin, and Carole Law.

GSC document code: GSC048

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG and the KPMG logo are registered trademarks of KPMG International, a Swiss cooperative.

© 2007 KPMG International. KPMG International is a Swiss cooperative. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved. Printed in the United Kingdom.
October 2007