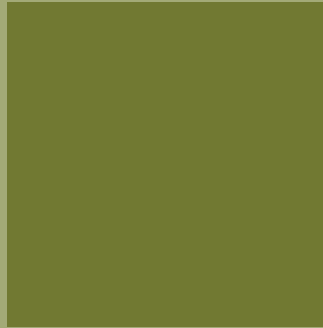


An aerial, high-angle photograph of a modern building's atrium. The space is characterized by a complex, multi-level design with white, curved architectural elements and a central, glowing yellow light fixture. The overall color palette is a mix of light and dark greens, with white highlights from the architecture and lighting.

Basel II – A Closer Look: Managing Operational Risk



Contents

1	INTRODUCTION
2	THE EVOLVING IMPORTANCE OF OPERATIONAL RISK
4	UNDERSTANDING OPERATIONAL RISK MANAGEMENT
9	OPERATIONAL RISK AND BASEL II
12	AN APPROACH TO MANAGING OPERATIONAL RISK
18	A PROCESS FOR ONGOING MANAGEMENT
20	DEVELOPING A SYSTEM FOR MANAGING OPERATIONAL RISK
22	CONCLUSION
23	ENDNOTES

Introduction

Deregulation and globalisation of financial services, along with the growing sophistication of financial technology, have created a variety of new operational risks for banks. Such risks arise from factors including:

- ▶ Increasing use of automated technology
- ▶ Growing importance of IT integration and shared services across entities
- ▶ Necessity of reducing earnings volatility and achieving cost efficiencies
- ▶ Increasing complexity of products and product development
- ▶ Increasing customer demands
- ▶ Increasing large-scale mergers and acquisitions
- ▶ Evolving outsourcing arrangements
- ▶ Proliferating complex credit and market risk mitigation techniques (such as derivatives)
- ▶ Increasing focus by regulators on legal, fraud, and compliance issues

To address such business issues adequately, banks face a growing need for better operational risk management. In addition, the Basel II Capital Accord requires banks to focus in a formalised, comprehensive manner on the operational risks that can result from external influences. What's more, rating agencies are now making a bank's operational risk management approach part of the rating decision.

As banks respond to these developments, many have discovered that, compared with the familiar territory of market and credit risks, operational risk affects the entire organisation, and its assessment is considerably more qualitative and subjective. Operational risks are often not clearly discernible from market and credit risks. Moreover, banks may have the impression they manage operational risks already, a perception that may prove only partly accurate. As a result, identifying and assessing such risks, and then managing them properly, is a highly complex and difficult endeavour.

Although many bank leaders have recognised the significance of evolving operational risks, many do not yet perceive them as a distinct class of risks or fully understand the business benefits banks can derive from a comprehensive, consistent approach to operational risk management. Basel II brings new urgency to the issue by asking banks to implement an enterprise-wide risk management framework that encompasses operational risks.

With this white paper, we emphasise the importance of banks' ongoing efforts to manage operational risks—efforts that can help them add value to the business as well as comply with Basel II.

Jörg Hashagen
Head of KPMG's Basel Initiative

The Evolving Importance of Operational Risk

Often difficult to perceive, quantify, and manage, operational risk poses some of the greatest challenges banks face today. Indeed, some of the industry's most experienced leaders have seen their institutions suffer severe losses attributable to operational risk, and yet for years many banks have misunderstood its significance or neglected its management. Some have believed they were already sufficiently managing operational risks—because they had taken steps to guard against fraud or other high-impact/low-probability events—but were actually failing to manage the everyday operational risks that over time can eat away at earnings, profitability, and reputation (see *Figure 1*).

Old perceptions and behaviours are beginning to change, however, as operational risk management has acquired new credibility as a means of adding value to the business and has garnered new attention from regulators and other key stakeholders.

Two important developments are driving the change. First, banks are recognising that a consistent and effective operational risk management programme can help them achieve organisational objectives. For example, by including a well-constructed operational risk process in the strategic, business, and product development processes, a bank can help ensure that the risks inherent in those activities are understood and addressed. In many instances the early involvement of operational risk management can increase the development speed of these new initiatives.

Moreover, many banks acknowledge that traditional risk management approaches fall short of providing senior management with a comprehensive picture of operational risk and therefore often fail to prevent severe losses. Such approaches address operational risk components in largely discrete ways—through, for example, internal control enhancements, performance improvement programmes, insurance, outsourcing, or internal audit. Often unconnected and inconsistent, these methods therefore tend to be only partly effective.

Banks are recognising that an effective operational risk management programme can help them achieve organisational objectives.



The second key development is the launch of the Basel II Capital Accord (the New Accord) by the Basel Committee for Banking Supervision. As of 2007, the New Accord will require banks to set aside regulatory capital for operational risk—an important development that affects most financial services institutions worldwide.

As operational risk management has evolved as a means of adding business value, banks have begun to perceive operational risks as constituting a separate risk category to be managed as part of overall corporate governance. Thus, as Basel II's 2007 deadline approaches, banks and other financial institutions are focusing on the strategic implications and opportunities presented by the New Accord's risk focus as well as preparing for compliance.

This document describes the growing importance of treating operational risk as a separate category of risks whose importance for banks is generally greater than market risk and, indeed, rivals credit risk. It discusses how and why—quite apart from the mandates of Basel II—banks are taking new steps to measure and manage this increasingly important array of risks. This document also describes evolving industry developments as well as Basel II's requirements, and it suggests an approach banks can use to address the issues and challenges associated with operational risk management.

Figure 1: What Is Operational Risk?

Operational risk is defined by the Basel Committee as “the risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events” including legal risk but excluding strategic and reputational risk.¹ (Although many banks consider reputational risk to be of considerable importance and a key aspect of their risk management efforts, it is often seen as secondary, caused by credit, operational, or market risk. This paper focuses on those risks the Basel Committee defines as operational.) Examples of operational risks are listed below:

Business Area	Potential Risks
Processes	<ul style="list-style-type: none"> ▶ Breach of mandate ▶ Incorrect/untimely transaction capture, execution, and settlement ▶ Loss of client assets ▶ Mis-pricing ▶ Incorrect asset allocation ▶ Compliance issues ▶ Corporate action errors ▶ Stock lending errors ▶ Accounting and taxation errors ▶ Inadequate record-keeping ▶ Subscription and redemption errors
People	<ul style="list-style-type: none"> ▶ Unauthorised trading ▶ Insider dealing ▶ Fraud ▶ Employee illness and injury ▶ Discrimination claims ▶ Compensation, benefit, and termination issues ▶ Problems recruiting or retaining staff ▶ Organised labour activity ▶ Other legal issues
Systems	<ul style="list-style-type: none"> ▶ Hardware and/or software failure ▶ Unavailability and questionable integrity of data ▶ Unauthorised access to information and systems security ▶ Telecommunications failure ▶ Utility outage ▶ Computer hacking or viruses
External Events	<ul style="list-style-type: none"> ▶ Operational failure at suppliers or outsourced operations ▶ Fire or natural disaster ▶ Terrorism ▶ Vandalism, theft, robbery

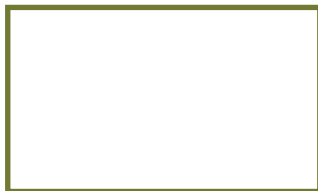
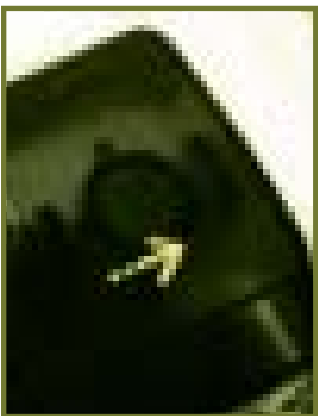
Source: KPMG, 2003.

Understanding Operational Risk Management

The banking industry's awareness of operational risk and efforts to manage it have accelerated in recent years, driven in part by an increasing desire to improve operating efficiency, reduce earnings volatility, and rationalise the allocation of capital between competing business uses. As operational risk management has evolved as a business management methodology, however, its development has been slowed by a number of obstacles.

Operational processes seem to have been generally well managed for many years, with just a few high-profile exceptions becoming public. Thus, banks and others are largely unclear on what specific benefits may accrue to an individual business unit from investment in operational risk management tools and methodologies. This apparent lack of tangible evidence of the current cost of operational risk can be explained, to a degree, by the distributed nature of its impact—that is, unlike credit and market risk, the impact of operational risk is often not felt in one account only, and it may not appear as a tangible loss at all. Consequently, broad-scale, enterprise-wide business buy-in for operational risk initiatives has proved slow to develop.

Regulators have not been quick to provide clarity on the issue, although Basel II is reinvigorating their focus. Having relied on bank management to determine their own approaches to operational risk, regulators are now endeavouring to learn more about these risks and their management as quickly as possible and are beginning to define some broad-based standards.



Challenges in Managing Operational Risk

Questions remain regarding how to identify and measure operational risk as well as which activities should be within the scope of formal operational risk management. Some banks have overcome their initial uncertainty as they have begun to develop an understanding of how operational risk management can add value to the business and as they have experienced external scrutiny (from regulators, shareholders, and other stakeholders, such as rating agencies). In general, banks' efforts have been effective if they have focused on some prerequisites for effective operational risk management, such as those described below:

Organisational Sponsorship

Implemented appropriately, operational risk management can add value to the business by, for example, increasing transparency of business performance, enhancing cost controls, and reducing earnings volatility. If, however, a bank's top leaders perceive operational risk management solely as a regulatory mandate, rather than as an important means of enhancing competitiveness, they may tend to be less supportive of such efforts. That inattention ultimately derails those efforts' chances for success. Management and the board must understand the importance of operational risk, demonstrate their support for its management, and designate an appropriate managing entity and framework—one that is part of the bank's overall corporate governance framework.

Business Line Buy-in and Resources

Business managers are wary of corporate initiatives that impose resource and time costs on the business but return few tangible business-level benefits. The business lines must be made aware that, in exchange for their participation in the development of an effective operational risk framework, they will obtain a consistent, bank-wide perspective on operational risk. As a result, they could benefit from understanding more about these risks, their costs to the business, and how the business can better align its mix of risks and rewards with the existing operating environment. A well-structured operational risk function can help enable operational risk management to add value and accelerate other processes. Indeed, effective management of operational risk could ultimately reduce the burden of required regulatory and economic capital. Over time, it can help drive operational efficiencies, cost reductions, better customer service, and other important goals.

Coordination with Existing Control Initiatives

Operational risk frameworks and implementation plans need to be coordinated with the bank's existing control framework efforts. These efforts may include risk assessment review processes; internal audit efforts; or compliance with International Financial Reporting Standards, the Sarbanes-Oxley Act of 2002, and other regulatory control requirements. Commonly used control frameworks share features with many of the essential steps in the operational risk framework, particularly with regard to risk identification and mitigation.

Development of Loss Databases

A well-structured operational risk framework requires development of business-line databases to capture loss events attributable to various categories of operational risk. Regulators expect internal loss databases to be comprehensive and to include several years of data prior to formal approval for use in the risk-estimation process. Basel II specifically requires a minimum of three years of data for initial implementation and ultimately five years for the Advanced Measurement Approaches (AMA). The need for historical data (including external data) has been a driving force behind efforts of many institutions to get their databases operational as soon as possible.

Well-Designed Methodologies and Models

Unlike market risk and credit risk quantification tools, operational risk tools are still at a relatively early stage of development, and market consensus has not yet converged on a set of "accepted" approaches for risk quantification. Nonetheless, many banks do tend to combine loss data modelling with results from qualitative risk assessments.

The loss database of a single financial institution may not contain sufficiently granular data to support statistically meaningful estimates of operational loss. To provide banks with more extensive data, efforts are under way within the industry to pool loss data among institutions and allow participating banks to share industry loss data. While this approach may result in a more densely populated loss database, individual banks may find it challenging to scale broad-based industry data to the specific risks of their lines of business.



Access to Appropriate Information and Reporting

Effective management of operational risk requires diverse information from a variety of sources—including, for example, risk and control profiles, operational risk incidents, key risk indicators, and rules and definitions for regulatory capital and economic capital reporting. To meet operational risk management requirements, two levels of performance metrics are evolving—one focused on meeting regulatory reporting requirements, and another used as part of the business’s ongoing cost containment, capital allocation, and process improvement initiatives.

To provide business managers with some immediate benefits from their investments in an operational risk methodology, some banks have emphasised the development of business-level operational risk metrics and economic capital allocation and reporting processes. At a number of institutions, these reporting tools have already enhanced business decision-making processes at both the business unit and the entity-wide levels.

Mistaking Operational Risk for Market or Credit Risk

Critics who object to the treatment of operational risk as a distinct risk type argue that major consequences will ultimately show up in the credit or market risk buckets. This view is still widely shared, but it is also misleading from a management perspective. These risks have structural differences in almost every aspect—including (as shown in *Figure 2*) inspection level, maximum loss amount, and portfolio—and therefore require different responses from management. Overlooking key events or misclassifying operational risks as market or credit risks can have considerable consequences for banks, as described below.

Figure 2: Structural Differences Among Risks

Managing operational risk differs from managing market or credit risk because operational risk affects every activity and process in a financial institution. Consequently, the responsibility for its management cannot be fully centralised but must take place both at the group/corporate level and within the business lines, as described herein.

	Market	Credit	Operational
Inspection level	Trading desk/portfolio	Credit portfolio	Business line
Risk categories	Interest/FX	Segments	Loss-event categories
Portfolio elements	Securities	Credits	Processes
Maximum total loss	Market value (excluding short sales/derivatives)	Credit volume	Bank’s liquidation value
Maximum number of losses	Number of securities	Number of credits	Unlimited

Source: KPMG, 2003.

Market Risk and Operational Risk

Examples of operational risk loss-events that manifest themselves in market risk include (1) market losses resulting from trading products for which the broker had no authorisation and (2) unwanted positions resulting from the inappropriate entry and acceptance of orders into electronic trading systems. The closing of such positions can result in losses (or even wins) should prices change in the meantime. Such events are assigned to the operational risk category and are entered in the loss data pool to provide a sound basis for future management decisions.

Credit Risk and Operational Risk

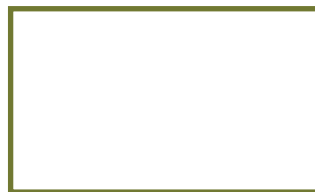
A large number of losses traditionally associated with a company's credit business do not result from an actual credit risk but from an operational risk. One example is a defaulted credit in the wake of a mismanaged loan-granting procedure that results in the assignment of an incorrect rating or the incorrect overwriting of an automatically assigned rating. Another example of a loss incurred due to operational risk has its roots in the mismanagement of collaterals, such that, in the wake of a default, reducing the risk position to the extent expected proves impossible.

In many cases, an event may be assigned to several risk types. If a severe operational risk event is accounted for under credit risk, the loss may very well be reported, and the economic capital number may even be adjusted to ensure appropriate capital coverage. However, the wrong data or assumptions are unlikely to lead to appropriate management decisions. The resulting (incorrect) credit risk increase will almost certainly result in a reduction of loans in a region or to an industry sector or client—but seldom will result in the credit process redesign that is likely needed. Management needs to understand the causes and the consequences of their risks to manage them appropriately.

Operational Risk and the Regulators

Apart from the business benefits banks derive from operational risk management, Basel II has given them new impetus to focus on these risks. Indeed, "Just as operational risk looked like it might be a delinquent, a disciplinarian arrived in the guise of the Basel Committee to give structure in the form of the proposal on a New Capital Accord. With the authority of the Basel Committee behind it, operational risk managers could start in earnest on establishing an operational risk management framework."²

The next section, beginning on page 9, describes how Basel II's operational risk focus and new mandates have prompted banks to pay increased attention to these risks and their management.



Operational Risk, New Regulation, and Corporate Governance

The Basel Committee has asserted, “The most important types of operational risk involve breakdowns in internal controls and corporate governance.”³ In its focus on operational risk, Basel II aligns with a variety of other regulations and supporting frameworks the purpose of which is to enhance corporate governance.

For example, banks that must comply with Basel II will see similarities between its Pillar II Principle 1 and, for example, the internal controls framework developed by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission in the United States—a framework that many organisations are using in complying with certain aspects of the Sarbanes-Oxley Act (S-O) of 2002. Banks may also see similarities in:

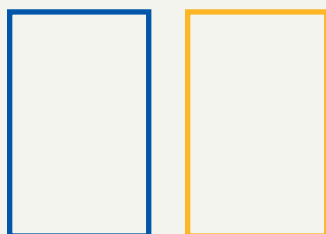
- ▶ The framework developed by the Canadian Institute of Chartered Accountants’ Criteria of Control (CoCo) Committee
- ▶ The United Kingdom’s Financial Services Authority (FSA) requirements and the governance standards set out in the Combined Code
- ▶ The Dutch Regulation on Organisation and Control (ROC) of the Dutch Central Bank and the Nadere Regeling 2002 of the Financial Markets Authority
- ▶ The German Corporate Sector Supervision and Transparency Act (KonTraG) and Section 25a of the German Banking Act (KWG)

Although their origins vary, these regulations/frameworks all seek to encourage or require incentives for improved risk management and internal control and, thereby, good corporate governance. For example, KWG Section 25a and KonTraG in Germany as well as the U.K.’s FSA Handbook emphasise senior management’s overall responsibility for risk management and suggest that all staff members be aware of their risk management responsibilities. S-O establishes clear standards for management’s accountability and dictates consequences for non-compliance. COSO and CoCo, among others, provide integrated frameworks for internal control, with risk assessment playing an integral role. Nevertheless it’s important to note that the existing rules and regulations predominantly focus on financial reporting and financial controls.

Basel II’s operational risk requirements could significantly broaden this focus as operational risk management, by its very nature, forces corporate governance to focus on both non-financial reporting and non-financial controls.

The Basel Committee affirms that the means by which banks will share information publicly will depend on the legal authority of local regulators. Moreover, Basel II’s disclosure requirements (Pillar III) are intended not to conflict with the broader accounting disclosure standards with which banks must comply. For example, the Basel Committee and the International Financial Reporting Standards (IFRS) Board are currently seeking to harmonise the two standards, especially with regard to disclosures in the financial statements of banks and other financial institutions and financial instruments.

Enhanced disclosure, through Basel II and IFRS, is intended to improve the transparency of banks’ business and risk structures. It is also intended to provide banks with positive incentives to strengthen risk management and internal controls. Under Basel II, the quality of the individual design and implementation of a control framework will directly affect the bank’s capital charge—consequently, governance quality becomes a function of cost of capital. Sound operational risk management and heightened transparency are integral components of enhanced corporate governance.





Operational Risk and Basel II

Influenced by developments in industry business practices, the Basel Committee has recommended that operational risk be defined as an independent risk category that must be backed by regulatory capital. The Basel Committee first demonstrated its interest in operational risk with a 1998 paper entitled, *Operational Risk Management*, in which it said that “managing such risk is becoming an important feature of sound risk management practice in modern financial markets.”⁴

Later, in the initial consultation paper describing the new regulations for banks’ equity capital requirements, the Basel Committee announced its deliberations for prescribing equity capital requirements for “other risks, including...operational risk.”⁵ The EU Commission has also indicated its support for this development.⁶

However, not until operational risk became part of that first draft of the consultative process from which emerged Basel II did the subject appear on the agenda for the majority of senior managements. In February 2003, the Basel Committee issued *Sound Practices for the Management and Supervision of Operational Risk*, in which it sought to provide guidance (see sidebar on page 11).

By including operational risk in its proposals for a new regulatory framework, the Basel Committee acknowledged the emerging importance of a sound operational risk management function. Moreover, it also underscored that failing to develop such a framework will continue to cost banks additional money due to operational risk events that could be prevented.

Basel II’s Approaches to Operational Risk

With Basel II, the Basel Committee provides a continuum of three approaches for the calculation of the minimum capital requirements necessary to cover operational risk (summarised in *Figure 3* on page 10):

- ▶ Basic Indicator Approach
- ▶ Standardised Approach
- ▶ Advanced Measurement Approaches (AMA)

By providing a range of approaches, the Basel Committee sought to allow banks and their regulators to select the one most appropriate to a bank’s size, the complexity of its operations, and the nature of its risks. In principle, the assessment procedures become increasingly sophisticated and consequently increasingly risk-sensitive and stringent in their qualitative and quantitative requirements. Competitive dynamics, regulatory pressures, and other factors will affect the choice of approaches.

The prospect of capital reductions is an incentive for banks to use the AMA. Furthermore, regulators have proposed the “partial use” of sophisticated approaches (that is, the possibility of applying these approaches to selected business areas), subject to the fulfilment of certain prerequisites.

Figure 3: Basel II's Operational Risk Approaches

Approach	Basic Indicator Approach	Standardised Approach*	Advanced Measurement Approaches (AMA)
Calculation of Capital Charge	<ul style="list-style-type: none"> ▶ Average of gross income over three years as indicator ▶ Capital charge equals 15 percent of that indicator 	<ul style="list-style-type: none"> ▶ Average gross income over three years per regulatory business line as indicator ▶ Depending on business line, 12 percent, 15 percent, or 18 percent of that indicator as capital charge ▶ Total capital charge equals sum of charge per business line 	<ul style="list-style-type: none"> ▶ Capital charge equals internally generated measure based on: <ul style="list-style-type: none"> - Internal loss data - External loss data - Scenario analysis - Business environment and internal control factors ▶ Recognition of risk mitigation (up to 20 percent possible)
Qualifying Criteria Compliance with the Basel Committee's "Sound Practices for the Management and Supervision of Operational Risk" recommended for all approaches.	<ul style="list-style-type: none"> ▶ No specific criteria 	<ul style="list-style-type: none"> ▶ Active involvement of board of directors and senior management ▶ Existence of OpRisk management function and independence of that function ▶ Sound OpRisk management system ▶ Systematic tracking of loss data 	Same as Standardised, plus: <ul style="list-style-type: none"> ▶ Measurement integrated in day-to-day risk management ▶ Review of management and measurement processes by internal/external audit ▶ Numerous quantitative standards—in particular, 3–5 years of historic loss data

Source: KPMG, 2003.

*Subject to regulatory approval, an "Alternative Standardised Approach" based on loans and advances instead of gross income can be allowed for certain business lines.

Moreover, large banks can expect that regulators will likely want to see them move in a structured way toward the use of the advanced approaches. To meet that goal, banks will need to develop and use models that are acceptable to regulators. Appropriately designed and implemented, such models can enable banks to measure and monitor risks across the organisation, enhance risk management, and ultimately determine capital requirements. *Figure 3, Basel II's Operational Risk Approaches*, summarises the criteria for the three approaches and the effort required of banks to fulfil them.

From Theory to Practice

Whatever approach an organisation adopts, implementing a robust operational risk management framework requires an integrated risk management process supported by consistent methodologies and infrastructure. Relying on existing structures, methods, and tools may not be sufficient because they often

lack the necessary consistency and homogeneity. Developing and implementing appropriate policies and infrastructure requires the sponsorship of management and the buy-in of the business lines as well as an appropriate commitment of resources. Personnel across the organisation must be educated in the complexities of operational risk and its management, and management must clarify roles and responsibilities. Internal audit, especially, should be involved in the independent review of the overall operational risk management framework.

The next two sections, beginning on pages 12 and 18, respectively, describe the elements of an operational risk framework and an ongoing process banks can use in managing operational risk across the institution. The section that follows addresses an approach management can use to develop such a process.

“Sound Practices” for Managing Operational Risk

The components for an overall operational risk framework have begun to emerge in the banking community. Some disagreement exists on the details of the approach and implementation process. Due to the complexity of today’s financial services companies, senior management needs to distinguish between mandatory components to be implemented regardless of size, business, and products and the bank-specific aspects of development, including the implementation approach and specific deviations in methods and tools.

The Basel Committee acknowledges the difficulty of developing a framework for operational risk, but it has sought to provide incentives for banks to continue to develop such frameworks. To provide common ground, the Basel Committee developed a guideline document, “Sound Practices for the Management and Supervision of Operational Risk.” The document provides no detailed road map but on a generic level encompasses the elements necessary to establish a sound framework.

In “Sound Practices,” the Basel Committee noted that:

“... management of specific operational risks is not a new practice; it has always been important for banks to try to prevent fraud, maintain the integrity of internal controls, reduce errors in transaction processing, and so on. However, what is relatively new is the view of operational risk management as a comprehensive practice comparable to the management of credit and market risk in principle, if not always in form. [Developing economic trends], combined with a growing number of high-profile operational loss events worldwide, have led banks and supervisors to increasingly view operational risk management as an inclusive discipline, as has already been the case in many other industries.”

“Sound Practices” can also be seen as another step in articulating comprehensive rules for corporate governance for all major risk types (following, for example, the MaH and MaK guidelines issued by German banking supervisors on market and credit risk policies respectively, Turnbull in the United Kingdom, and COSO in the United States as well as similar frameworks in other countries). The paper encompasses ten principles for the effective management and supervision of operational risk. These principles reflect:

- Activities many financial institutions have been successfully developing over the years as part of their operational risk frameworks
- The current thinking of supervisory regimes on Basel II, highlighting the importance placed on the New Accord’s Pillars II and III



The Ten Principles of the Basel Committee’s “Sound Practices”

The ten principles concentrate on the high-level standards deemed necessary for the management of operational risks.⁹ In keeping with the Basel Committee’s goals, the principles are deliberately high-level to allow banks to develop approaches suitable to their organisational needs.

The ten principles can be summarised as follows:

- The board of directors and senior management are responsible for approving the establishment and review of a framework for managing operational risk and establishing the organisation’s operational risk strategy.
- Senior management is responsible for implementing the operational risk strategy consistently throughout the entire organisation and developing policies, processes, and procedures for all products, activities, processes, and systems.
- Information, communication, and escalation flows must be established to maintain and oversee the effectiveness of the framework and management performance.
- Operational risks inherent in all current activities, processes, systems, and new products should be identified.
- Processes necessary for assessing operational risk should be established.
- Systems should be implemented to monitor operational risk exposures and loss events by major business lines.
- Policies, processes, and procedures to control or mitigate operational risks should be in place, together with cost/benefit analyses of alternative risk limitation and control strategies.
- Supervisors should require banks to have an effective system in place to identify, measure, monitor, and control operational risks.
- Supervisors should conduct (directly or indirectly) regular independent evaluations of these principles and ensure that effective reporting mechanisms are in place.
- Sufficient public disclosure should be made to allow market participants to assess an organisation’s operational risk exposure and the quality of its operational risk management.

An Approach to Managing Operational Risk

An approach to managing operational risk should consider (1) what activities or components are to be created, enhanced, and managed; (2) who should manage these interrelated activities, entity-wide and within the business units; and (3) how those responsible may go about the process.

An Operational Risk Framework

The framework approach illustrated in *Figure 4* and described below provides a way to structure the challenge of what to manage. The section *A Process for Ongoing Management*, beginning on page 18, describes an approach to the management of such a framework.

Figure 4: A Framework for Managing Operational Risk



Source: KPMG, 2003.

Risk Strategy

A bank's strategy for operational risk drives the other components within the management framework. It also has to provide clear guidance on risk appetite or tolerance, policies, and processes for day-to-day risk management.

Thus the operational risk strategy comprises both the "top-down" process of capital allocation and clear guidance for the "bottom-up" processes of risk identification, assessment, management, reporting and supervision, and governance arrangements that constitute the management framework. Each business unit's management has to comply with the bank's overall risk strategy when making business decisions based on the available operational risk information, while considering overall capital requirements.

The terms *risk appetite* and *risk tolerance* are also commonly associated with risk strategy. Generally established "top down" by an organisation's board or risk committee, these measures have been used successfully in a market risk and credit risk context for years. However, many organisations are struggling to apply them "top down" to the management of operational risk, perhaps due to the breadth of such risk as well as the limitations inherent in current quantitative measures.

Instead, organisations tend to consider operational risk appetite and tolerance from a “bottom-up” perspective. Specifically, they apply thresholds by risk functions and/or business units to the various forms of operational risk information (risk assessment reports, key risk indicators, and the reporting and escalation of operational risk incidents and losses).

Additionally, many banks consider the appetite or tolerance for operational risk as part of the day-to-day management of the business—during new product approval, for example, or within change management processes. However, this piece-meal approach has limited value in that risk appetite and tolerance are not considered in an appropriately broad, formalised context.

Organisational Structure

The organisational structure is the bank-wide foundation for all operational risk management activities. Within this context, the bank defines and assigns centralised and decentralised roles and responsibilities to a wide array of organisational units, functions, and, ultimately, individuals. For some banks, these roles and responsibilities will be new.

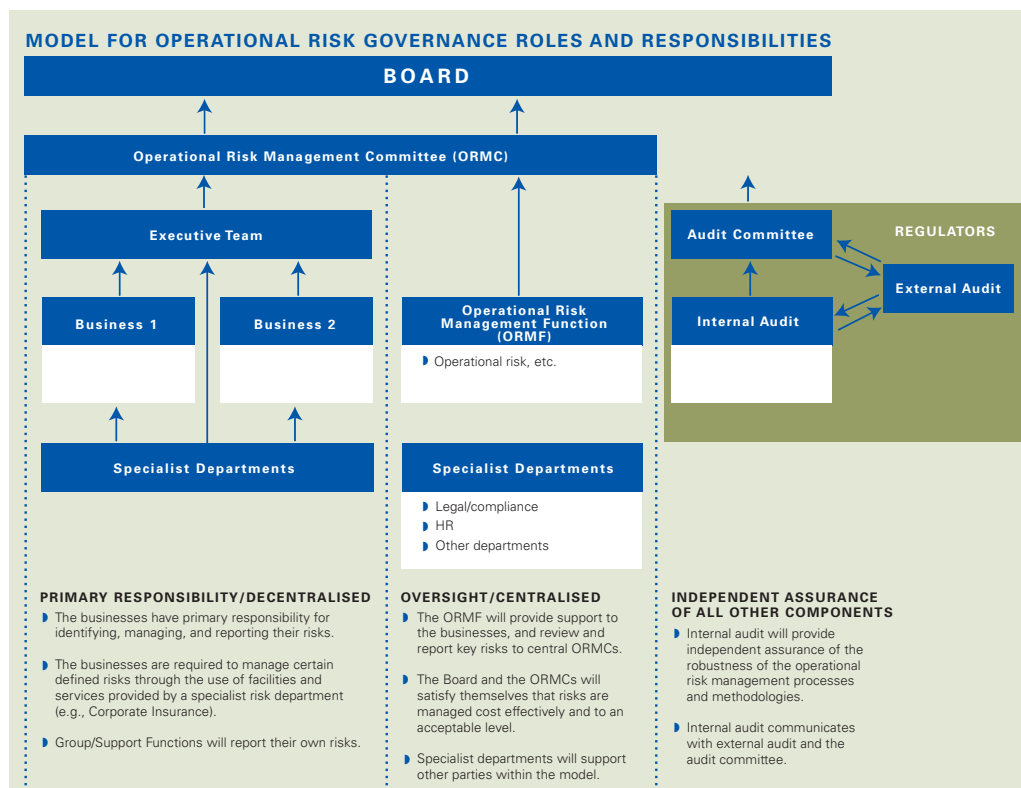
With market and credit risk management serving as role models, two key goals need to be reflected in an organisational structure for operational risk:

- ▶ The agreement that operational risk cannot be confined to specific organisational units (unlike market risk) but remains largely the responsibility of line managers and some defined special or support functions (such as IT, HR, legal, internal audit, or compliance); and
- ▶ The division of duties among management, an (often to be established) independent risk management function, and internal audit.

The organisational structure also comprises reporting lines, both at the entity-wide level and within the business units (see *Figure 5*). The organisational structure links operational risk management performance to business targets and employee performance goals. It encompasses escalation processes and procedures and operational risk policies, and is closely aligned with the operational risk strategy.

When designing the operational risk management organisational structure, the bank’s overall risk management structure should serve as a guideline. The desired end state should be to serve global risk management needs.

Figure 5: Potential Organisational Model



Operational risk management requires the attention and involvement of a wide variety of organisational constituencies, each of which has different responsibilities and expectations. Critical to the effort’s success are centralised and decentralised operational risk management teams, which are responsible for implementation at the group/corporate and business unit levels, respectively.

Source: KPMG, 2003.

Even with an emerging industry practice, experience has shown two special issues for consideration:

- ▶ Treatment of the specialist functions (provide IT, HR, or legal risk management functions or independent oversight)
- ▶ The role of a (likely new) operational risk committee (as a body of its own or a subgroup of an overall risk committee)

All these issues will have to be documented in operational risk policies that are closely aligned to the operational risk strategy.

Reporting

Because operational risk affects all business units, operational risk management reporting has a much broader scope than traditional market or credit risk reporting (see *Figure 6*). Such reporting has to cover two distinct aspects:

- ▶ Delivery of defined, relevant operational risk information to management and risk control, and
- ▶ Reporting of information aggregated by risk category to business line management, the board and the risk committee.

Whereas the first type of information contains predominantly “raw” data such as losses, near misses, indicators, and risk assessment results, the second reflects aggregated, structured, and often analysed information designed to provide each level of management with what it needs to enable better operational risk management.

It is in the nature of operational risk that, parallel to regular reporting lines, the bank needs a reporting structure for severe events that ensures timely information and supports immediate measures by management.

Definitions, Linkages, and Structures

Banks need a common language for describing operational risk and loss-event types, causes, and effects. They also need to map the rules necessary for compliance with regulatory requirements. The development of definitions, linkages, and structures enables banks to efficiently identify, assess, and report such operational risk-related information. Definitions,

Figure 6: Operational Risk Management Reporting

Recipient	Type of Information Received
Board	<ul style="list-style-type: none"> ▶ Aggregated bank-wide information on loss data ▶ Risk assessment and key risk indicators results ▶ Economic and regulatory capital ▶ Ad hoc reports in case of major events
Operational Risk Management Committees	<ul style="list-style-type: none"> ▶ Aggregated bank-wide information on loss data ▶ Ad hoc and detailed reporting of major events ▶ Risk assessment and key risk indicators results ▶ Economic and regulatory capital
Business-Unit Heads	<ul style="list-style-type: none"> ▶ Aggregated business-unit-specific information on loss data ▶ Risk assessment and key risk indicators results ▶ Economic and regulatory capital ▶ Ad hoc reports in case of major events
Operational Risk Management Function	<ul style="list-style-type: none"> ▶ Detailed (raw) bank-wide information on loss data ▶ Risk assessments ▶ Key risk indicators
Specialist Departments	Detailed bank-wide information in the respective area of expertise
Audit Committee	According to actual information requirements
Internal Audit	According to actual information requirements
External Audit	According to actual information requirements
Regulators	<ul style="list-style-type: none"> ▶ Regulatory capital ▶ Operational risk losses

Source: KPMG, 2003.

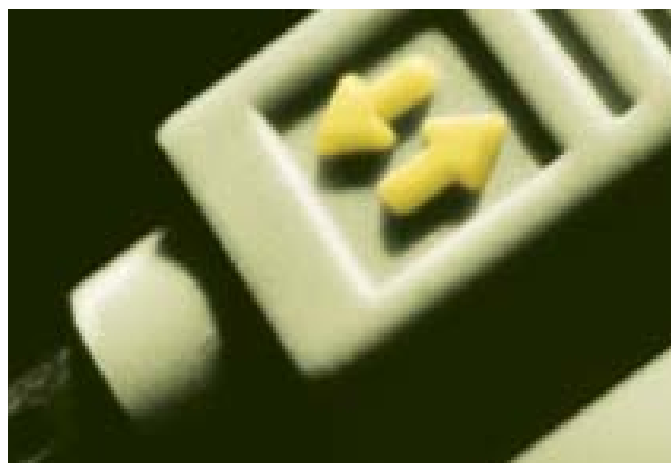
linkages, and structures thus form the basis of consistent databases that enable banks to maintain data that remains meaningful over time. The endeavour helps to clarify the scope of operational risk and avoid differing interpretations as well as identify sub-categories and boundaries with other areas of risk (especially credit and market). It also helps enable the mapping of underlying data to the Basel framework or other recognised control frameworks (such as COSO). Finally, comparisons between different sources of information (e.g., risk assessment, loss data collection, key risk indicators) can be conducted on a consistent basis, which leads to the ability to draw more powerful conclusions from the otherwise probably too-sparse data.

Major challenges arise in setting the boundaries between operational and other risk types, finding definitions that are understood throughout the bank, and coping with the effects of organisational restructuring efforts banks frequently undertake. Leading banks understand that keeping definitions, linkages, and structures up to date is crucial for the success of methods that are built upon them.

Loss Data

With a common language in place, the bank needs a process for collecting, evaluating, monitoring, and reporting operational risk loss data. Such a process would be designed to provide the basis for any management decision from ad hoc reporting to regular risk reporting and ultimately leading to support quantification models as well as risk assessments. In addition to implementing processes for collating internal loss data, the bank needs to consider in what way it wants to supplement it with external data—both publicly available or from data-sharing initiatives.

The collection of internal loss data requires the support of all areas of the bank. Loss events over a materiality threshold—potentially, but not necessarily, including indirect losses, foregone income, and near misses—need to be entered into a loss database and verified. Policies and procedures are needed to help ensure consistency and completeness. Changes to loss amounts, late insurance payments, and additional compensation claims have to be added in an auditable manner.



Low-frequency/high-impact losses (e.g., natural disasters, IT system breakdowns) are by definition usually not contained in an internal loss database because they may not have yet hit the organisation. Consequently, information on those losses has to be gathered externally. Public sources (i.e., press, news databases) are often useful, as is the anonymous sharing of internal loss data by member banks within a consortium.

Data availability and quality are often problematic. Just as a sound operational risk culture cannot be created overnight, the establishment of a loss data collection process takes time. After the successful implementation of an operational risk framework, the total number of events may decrease due to better management. Nonetheless, because scrutiny increases, the number of identified losses can also be expected to increase during the implementation phase of a comprehensive loss data collection process. Moreover, after such a process is established, results should be interpreted carefully. Some losses are detected only months or even years after their occurrence.

An internal loss data collection process should have a number of built-in incentives and controls to ensure a high degree of data coverage and quality. The internal loss data collection is enriched over time by both data sharing and external public data that are carefully screened and adjusted to enable a close resemblance to the bank's specific environment of processes, systems, and people.

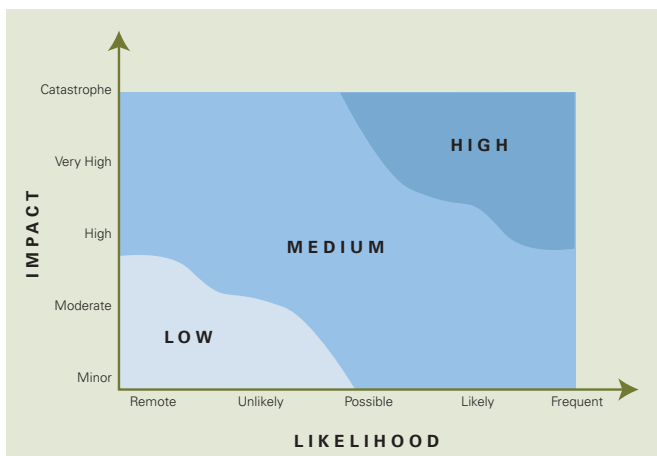
Risk Assessment

Risk assessment provides banks with a qualitative approach to identifying potential risks of a primarily severe nature by conducting structured scenarios with representatives of all business units.

As a tool that enables identification—and, to a limited extent, even quantification of operational risk—risk assessment picks up where loss data collection leaves off. Indeed, it helps fill the knowledge gap left by backward-looking and often sparse loss data and attempts to establish risk-sensitive and forward-looking identification of operational risk. While the details vary, the basic structure of a risk assessment is universal: a set of matrices identifying and assessing operational risk and its subcomponents in terms of likelihood and impact of occurrence, based on a defined risk appetite (see *Figure 7*).

The resulting risk profile presents a high-level overview of all risk areas per bank, business unit, or other aggregation level. More elaborate risk assessments differ among risk categories and inherent and residual risk and aim to assess the quality of risk-mitigating measures.

Figure 7: Risk Profile



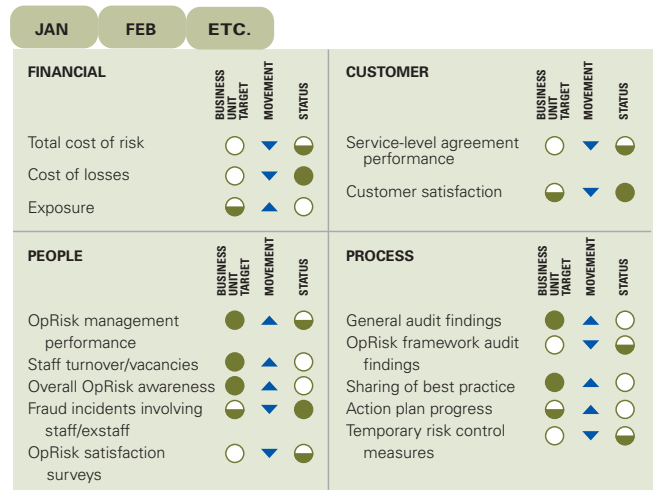
Source: KPMG, 2003.

Key Risk Indicators

The bank should assess aspects of operational risk based on key risk indicators (KRIs)—factors that may provide early warning signals on systems, processes, products, people, and the broader environment (see *Figure 8*).

Figure 8: Key Risk Indicators

A scorecard approach can assist in the assessment of various risks and how they change over time.



- Indicates immediate action required
- Indicates close monitoring needed
- Indicates no action required

Source: KPMG, 2003.

Like loss data, KRIs are based on existing data, such as certain ratios. Unlike loss data, however, KRIs do not look at the “face value” of information (assuming history may be repeated), but seek to predict certain future behaviour (for example, staff turnover—not representing actual losses but potential future losses should certain key personnel and knowledge be lost). Thus, KRIs differ from risk assessments in that they rely on observable data, not estimates of future activities.

Identifying relevant KRIs can be a complex endeavour, as the assumed correlation with actual exposure can only be determined over time using internal loss data. Banks may need to combine several primary or directly available indicators to achieve the desired early warning information. To maintain ease of comprehension, many banks have used only a limited set of generic indicators for business units across the bank along with an equally limited set of business-line-specific indicators where necessary.

Mitigation

Once the bank has identified and quantified its risks, it can implement a strategy for mitigating them with appropriate policies, procedures, systems, and controls. Within its established risk appetite and tolerance, the bank would retain a certain portion of risk, transfer another portion (through insurance), and then finance those risks it could not insure.

Risk mitigation is an iterative and ongoing process: as one tactic is implemented, others should be reassessed. Just as an investor adjusts the mix of investments based on defined targets for risk and return, a risk portfolio manager chooses among tactics to manage risk based on the bank's appetite for risk and its ability to absorb it. These choices can include adding controls or limits for risks that may exceed the bank's risk appetite. Such choices also may include reducing costs related to excessive controls or taking action to expand risks in areas where existing controls provide additional risk capacity. Thus the manager must continually balance the cost/benefit of taking such action with the need to mitigate risk in the organisation. By applying a variety of tactics, risk managers can begin to affect corporate performance and thereby affect shareholder value.

Capital Modelling

Capital modelling encompasses the calculation of regulatory and economic capital. It involves defining input data (internal and external loss data, scenario data, business environment, and control factors as well as auxiliary information such as insurance parameters), defining the mathematical/statistical relationships and assumptions for measuring operational risk, the implementation of the model, and the model validation.

Within the spectrum of approaches in Basel II, the AMA gives banks the flexibility to build their own models, taking into account their own structure, correlation and diversification effects, insurance mitigation, and other factors. The goal of capital modelling is to estimate expected losses, which should be taken into account in product pricing, as well as to calculate the Value-at-Risk for operational risk (unexpected losses) that have to be buffered by economic and regulatory capital. Those figures could then be integrated into a bank steering concept (Risk Adjusted Performance Measurement).

The key issue with capital modelling is the validation of input data, model structures, and assumptions as well as the validation of the model results. Often most challenging is the latter, where the benchmark is "events occurring less than once in a thousand years."

Currently three broad families of approaches are considered best practice: the loss distribution approach, the risk drivers and controls approach, and the scenario-based approach. As they are designed to help a bank qualify for an AMA, they make various uses of the four mandatory components—internal loss data, external loss data, scenarios, and business environment and controls factors.

Information Technology

Appropriate information technology is the foundation and facilitator of the operational risk management framework. The IT system will need to accommodate a wide variety of operational risk information, without the need for re-keying, and interface with a variety of internal systems as well as external sources. Users should be able to reconcile, enrich, maintain, and update information with source data. The central operational risk management function should consider how to store data and information and enable use of an intranet site. The framework should encompass the identification of business requirements and functional specifications for operational risk IT systems and vendor selection. Banks will need enhanced tools and techniques to meet new information requirements. Tools must enable the businesses to focus on key areas of risk.

Appropriate information technology is the foundation and facilitator of the operational risk management framework.

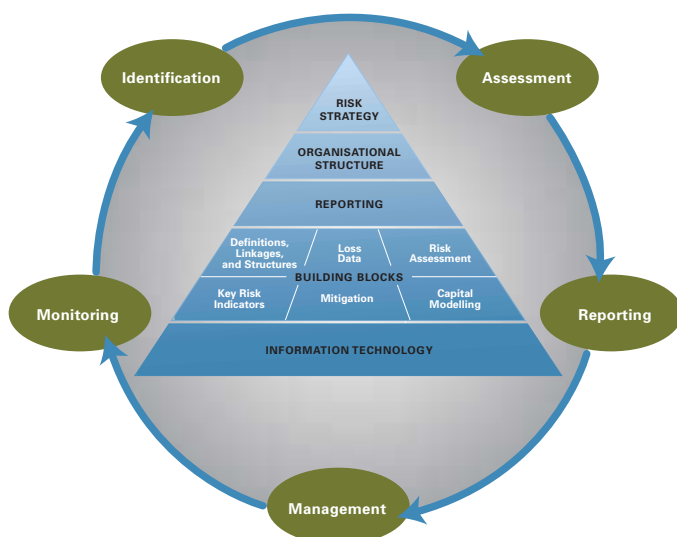
In general, implementing the data management and reporting systems required to optimise capital allocation not only releases resources to maximise return on capital but can also support a wide range of other business activities. The degree of data collection, data reconciliation, management, and reporting by Basel II (particularly in the area of operational risk) supports activities entity-wide—from, for example, maintaining the general ledger and enhancing human resources systems, to implementing a Customer Relationship Management programme.

A Process for Ongoing Management

The leaders responsible for the bank's governance process set the tone for how a bank implements and executes its operational risk management strategy. Operational risk management cannot become an effective process within the institution unless leaders articulate and support a high-level vision and business unit managers understand and appreciate the benefits they could derive from implementing the cultural and business process changes required by the new framework.

The management process for operational risk will likely resemble the processes employed for other risk areas, such as market risk or credit risk. Using the operational risk definitions, linkages, and structures; risk assessment; key risk indicators; and loss data base; the framework can provide management with relevant information to undertake a rigorous control programme. Such a programme is illustrated in *Figure 9* and described below.

Figure 9: A Process for Managing Operational Risk



Source: KPMG, 2003.

Identification

During the risk identification process, the bank's operational risk unit typically collects and uses a wide range of information, such as internal and external loss data, risk indicators, and output from risk assessment exercises. The operational risk unit analyses "near misses" and undertakes systematic analysis of processes and systems to consider risk potential for all defined operational risk categories. Concurrently, the individual business units use the same data to enhance their understanding of sources of business process error, areas of high expense, or inordinate work effort. Business units then perform their internal processes for identifying opportunities for improving operating efficiency.

Assessment

These internal processes include calculation of indirect losses, qualitative assessment of their risk potential, and evaluation using risk indicators. As the operational risk framework is being established, the individual business units participate with operational risk personnel in developing scenario analyses for identifying the frequency and consequences of potential risks. The scenarios are appropriate for the business unit and are modified over time as the business evolves and as the quality and quantity of business loss data become more robust. The

central operational risk management function can use scorecards to develop business-specific estimates of operational loss. These estimates are updated for each cycle of the operating risk reporting process.

Reporting

The analytic and data management efforts of the business and the operational risk team combine to develop reporting protocols that serve both the individual business and the central management team. The central operational risk team provides reporting that covers a “top-down” view of operational risk, including actual loss data, near misses, causes of loss and near miss, risk assessment, scenario data, and key risk indicators. The bank reports aggregate losses and trends, risk-assessment results, key risk-indicator results, and economic and regulatory capital to all relevant parties.

Reporting also should have a “bottom-up” perspective that is directed to the needs of the business unit management. These reports should be customised for the business unit to facilitate risk mitigation, process improvement, and cost containment.

Management

The operational risk management function uses the reporting process to identify key areas of process risk and trends in business behaviour. It works with senior management to identify firmwide efforts to prioritise risk mitigation strategies, including risk transfer, risk reduction, risk avoidance, and risk prevention. Entity-wide efforts to manage operational risk are coordinated with the efforts of the individual business units to implement specific risk management changes within the business units. To the extent that multiple business units face similar operational risk challenges, risk mitigation efforts for individual units may require cross-business coordination and collaboration.

Monitoring

The monitoring process is the capstone of the management process. Through this process the operational risk team and the business unit leaders are able to assess the effectiveness of their framework, identify areas of risk management weakness, and redirect the risk management effort to create a more robust control environment.

Figure 10: Stakeholder Roles and Challenges

Stakeholder	Roles and Responsibilities	Potential Challenges
Board	<ul style="list-style-type: none"> ▶ Affirm operational risk policy ▶ Sponsor focus on operational risk 	<ul style="list-style-type: none"> ▶ Inadequate or inaccurate information
Management	<ul style="list-style-type: none"> ▶ Develop operational risk policy ▶ Interpret new regulation ▶ Determine how to coordinate among centralised and decentralised risk management efforts ▶ Understand the impact of regulatory requirements on existing business practices ▶ Determine level of change required, associated costs, benefits and relevant options ▶ Build a robust business case for change ▶ Secure and maintain Board and senior management sponsorship and buy-in ▶ Implement change consistently across the organisation 	<ul style="list-style-type: none"> ▶ Absence of “standard” industry approaches and rapidly developing market ▶ Problems in implementing change consistently ▶ Lack of necessary resources
Specialist Departments	<ul style="list-style-type: none"> ▶ Collect data; report risks 	<ul style="list-style-type: none"> ▶ Lack of appropriate education, resources, training
Business Lines	<ul style="list-style-type: none"> ▶ Determine business requirements and sophistication of approaches required ▶ Embed new/enhanced practices into wider business environment ▶ Avoid gaps/overlaps in operational risk/credit risk approaches 	<ul style="list-style-type: none"> ▶ Lack of appropriate education, resources, training
Internal Audit	<ul style="list-style-type: none"> ▶ Review business line and centralised efforts to manage operational risk ▶ Link with external audit, audit committee 	<ul style="list-style-type: none"> ▶ Lack of appropriate education, resources, training

Source: KPMG, 2003.

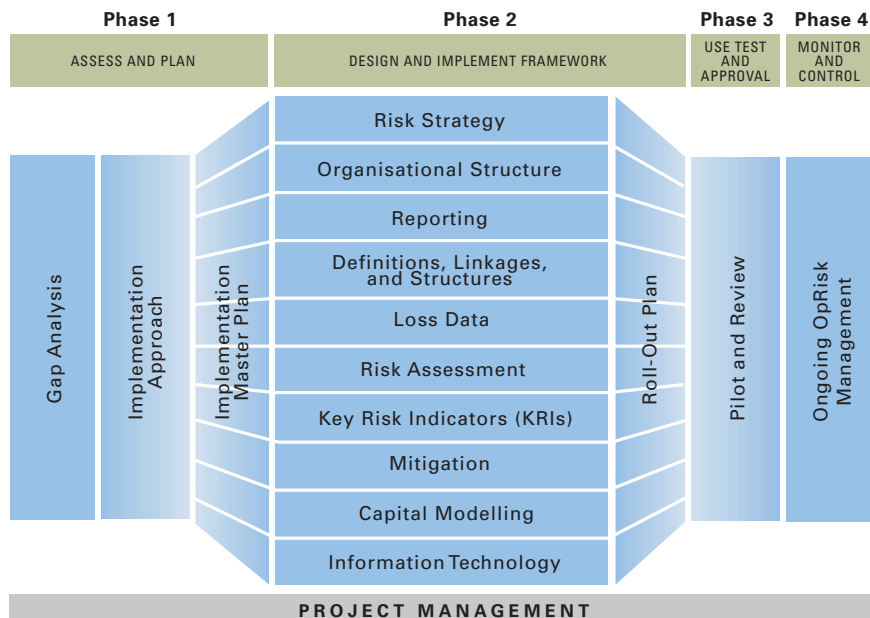
Developing a System for Managing Operational Risk

As shown in *Figure 10*, banks can take a phased approach to determining how to manage operational risk, who should be involved in its management, and what mechanism those people might use to maintain the process.

Phase 1 is an “as-is” analysis of a bank’s current operational risks process. During this phase the bank would evaluate how it presently manages operational risk, including the corresponding tasks and responsibilities. It would review the structure, content, and criteria of its current risk assessment approach. It would also review the frequency, audience, reporting structure, and escalation thresholds of its current risk reporting efforts. Analysis of existing key risk indicators and the processes that support data gathering is also part of this phase.

In **Phase 2**, the bank would establish various teams to address specific aspects of operational risk, including its organisational structure; definitions, linkages, and structures; loss data collection; risk assessment; key risk indicators (KRIs); reporting; capital modelling; and information technology. Teams focus on defining data needs; designing the organisational structures, processes, and systems, improving operational risk management; and rolling out the plan. Developing and executing a plan can help teams to address organisational considerations such as communications, training, and quality assurance.

Figure 11: A Phased Approach to Developing a System for Managing Operational Risk



Source: KPMG, 2003.

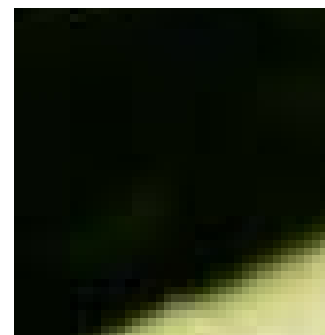
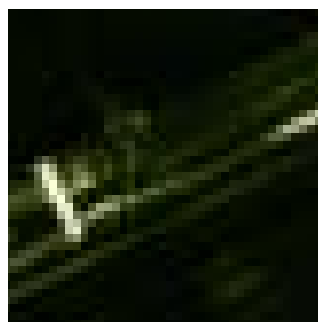
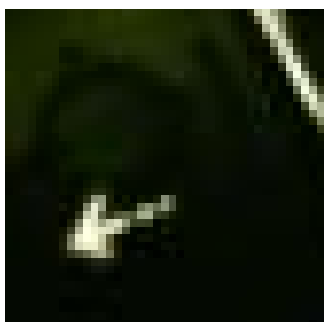
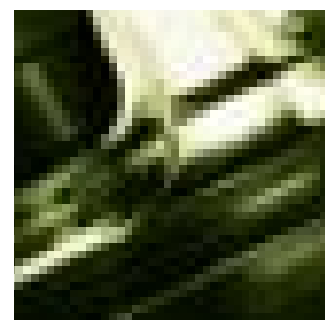
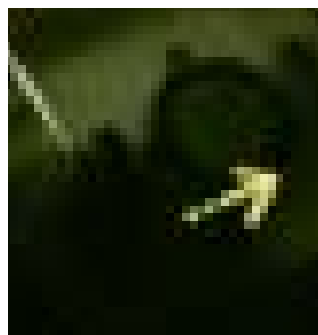
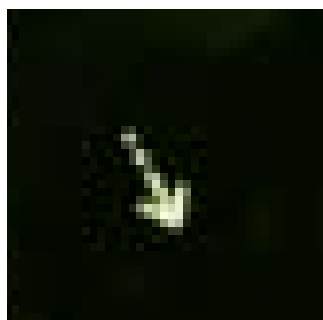
During **Phase 3** the bank would conduct a pilot of the approach, in which it can test its design in a small environment. The team revises the design based on the results, and then rolls it out within the organisation as a whole.

Ongoing operational risk management, **Phase 4**, is important both internally and externally. Banks will need to establish monitoring processes and systems that suit the needs of their own organisations and those of their regulators to develop a process that encompasses the five steps defined in *Figure 9* on page 18.

Although the duration of an operational risk project depends on the bank's individual circumstances, a full-fledged project may take two or more years. Given the Basel II requirements on internal loss data—which formulate a need for data history covering at least three years—a bank must address its organisational and data collection requirements immediately to be able to qualify for the AMA by the 2007 deadline. Indeed, such efforts are also critical to create a sufficient loss database to support adequate management decisions under every Basel II approach, except perhaps the Basic Indicator.

Why Operational Risk Management Efforts Can Fail:

- ▶ Lack of CEO and executive sponsorship
- ▶ Poor corporate culture and/or high-level control environment that is divorced from business objectives
- ▶ Unclear roles and responsibilities/organisational structures
- ▶ Poorly defined/inconsistent operational risk policy
- ▶ Undefined risk universe and no common risk language
- ▶ Poor/inconsistent operational risk identification process
- ▶ No linkage of risks to the control framework
- ▶ Over-engineered risk measurement and evaluation
- ▶ Reporting templates that do not integrate with business requirements
- ▶ Unclear escalation channels
- ▶ Poor action-tracking and project management systems
- ▶ Poor communication and education programmes



Conclusion

As banks have begun to manage operational risk as a means of adding business value, they have also begun to recognise that such efforts are a key aspect of effective corporate governance.

To achieve governance goals, management and the board need to take steps to understand the importance of operational risk, demonstrate their support for its management, and designate an appropriate managing entity and framework that are part of the bank's overall corporate governance framework. Basel II's

In managing operational risk, organisational and cultural issues ultimately pose greater challenges than the evolving technical hurdles that banks must overcome.

effective business case for operational risk management, leaders need to emphasise the business benefits that can result, rather than regulatory compliance requirements that

risk focus and the work required to meet its deadlines have also served to underscore the strategic implications and opportunities inherent in operational risk management.

In managing operational risk, organisational and cultural issues ultimately pose greater challenges than the evolving technical hurdles that banks must overcome. To build an

must be met. They need to consider the big threats (both operational and financial) that may affect the achievement of their strategic business objectives and how they can improve the timeliness, accuracy, and relevance of the risk information they collect. However, they also need to determine how they can protect and enhance value for stakeholders by improving operational performance and ensuring that they allocate and use capital in the most efficient and effective way.

Consistent, ongoing identification and management of relevant, meaningful, and comprehensive operational risk information are difficult undertakings, no matter how many resources are dedicated to these efforts. Risk assessment methodologies ultimately rely on the business lines' expert judgement to evaluate risk exposures and the effectiveness of the control environment. To be most effective, these methodologies should be applied within a robust operational risk management framework. Institutions need to devise appropriate incentive mechanisms that will help management establish, expand, and maintain a sound operational risk culture. In the short term, such efforts can help banks begin to comply with Basel II. Over time, they can also help banks add value to their businesses and enhance their corporate governance.

Endnotes

- ¹ BIS Sound Practices, February 2003, p. 2, paragraph 4.
- ² Roland Kennett. "How to Introduce an Effective Operational Risk Management Framework," *Advances in Operational Risk: Firm-wide Issues for Financial Institutions*, second edition, published in association with SAS, Risk Books, a division of Risk Waters Group Ltd., 2003, Chapter 5, pp. 73–92.
- ³ Basel Committee on Banking Supervision. "Operational Risk Management," September 1998, p. 1.
- ⁴ Basel Committee on Banking Supervision. "Operational Risk Management," September 1998, p. 3.
- ⁵ Basel Committee on Banking Supervision. "A New Capital Adequacy Framework," June 1999, p. 6.
- ⁶ "A Review of Regulatory Capital Requirements for EU Credit Institutions and Investment Firms," Consultation Document, European Commission Internal Market Directorate General, November 22, 1999.
- ⁷ Basel Committee on Banking Supervision. "Sound Practices for the Management and Supervision of Operational Risk," February 2003, p. 3.
- ⁸ Basel Committee on Banking Supervision. "Sound Practices for the Management and Supervision of Operational Risk," February 2003, pp. 4–5.



KPMG International

KPMG is the global network of professional services firms whose aim is to turn understanding of information, industries, and business trends into value. With nearly 100,000 people worldwide, KPMG member firms provide audit, risk advisory, tax and legal, and financial advisory services from more than 750 cities in 150 countries.

Major KPMG Contributors

Jörg Hashagen
Robert Antrobus
Ian Cottrell
Colleen Drummond
Azaan M. Jaffer
Thomas Kaiser
Marc Koehne
Carole Law
Ernst Lock
Bill Murphy
Diane Nardin
Mike Ritchie
Steven M. Roberts
John P. Somerville
Steve Whiting

Visit KPMG on the World Wide Web at www.kpmg.com.

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 endeavour 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 upon such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG International is a Swiss cooperative comprising separate KPMG member firms in countries throughout the world. All professional services are performed by KPMG member firms in their local regions and not all such firms perform the services set forth in this document. In addition, not all KPMG member firms are authorized to perform legal services, and those that are so authorized may do so only in their local regions.

© 2003 KPMG International. KPMG International is a Swiss cooperative of which all KPMG firms are members. KPMG International provides no services to clients. Each member firm is a separate and independent legal entity and each describes itself as such. All rights reserved. Printed in the United Kingdom. 25161atl

© 2003 KPMG International. KPMG International is a Swiss cooperative of which all KPMG firms are members. KPMG International provides no services to clients. Each member firm is a separate and independent legal entity and each describes itself as such. All rights reserved.

KPMG's Basel II Contacts

Head of KPMG's Basel Initiative

Jörg Hashagen
Tel: +49 69 9587 2787
E-mail: joerghashagen@kpmg.com

Argentina

Maria G. Saavedra
Tel: +54 11 4316 5860
E-mail: gsaavedra@kpmg.com.ar

Australia

John Somerville
Tel: +61 3 9288 5074
E-mail: jsomerville@kpmg.com.au

Austria

Gerhard Feiler
Tel: +43 1 31 332 280
E-mail: gfeiler@kpmg.at

Belgium

Stéphane Darimont
Tel: +32 2 708 4701
E-mail: sdarimont@kpmg.com

Brazil

Ricardo Anhesini
Tel: +55 11 3067 3141
E-mail: rsouza@kpmg.com.br

Canada

Azaan Jaffer
Tel: +1 416 777 8500
E-mail: amjaffer@kpmg.ca

Croatia

Janez Uranic
Tel: +385 1 466 6440
E-mail: janez.uranic@kpmg.hr

Czech Republic

Vladimir Dvoracek
Tel: +420 222 123 117
E-mail: vdvoracek@kpmg.cz

Denmark

Merete Lykke Rasmussen
Tel: +45 3818 3151
E-mail: mlrasmussen@kpmg.dk

Finland

Raimo Saarikivi
Tel: +358 9 6939 3703
E-mail: raimo.saarikivi@kpmg.fi

France

Vicky Papaevangelou
Tel: +33 1 5568 7114
E-mail: vpapaevangelou@kpmg.com

Germany

Klaus Ott
Tel: +49 69 9587 2684
E-mail: kott@kpmg.com

Greece

Nick Vouniseas
Tel: +30 210 6062 114
E-mail: nvouniseas@kpmg.com

Hong Kong/China

Martin Wardle
Tel: +852 2826 7132
E-mail: martin.wardle@kpmg.com.hk

Hungary

John Varsányi
Tel: +36 1 270 7200
E-mail: john.varsanyi@kpmg.hu

India

Joy Uka
Tel: +91 22 2491 3030
E-mail: juka@kpmg.com

Indonesia

Kusumaningsih Angkawidjaja
Tel: +62 21 574 2333
E-mail: kangkawidjaja@siddharta.co.id

Iran

Ali Reza Jam
Tel: +98 21 830 7928
E-mail: ajam@kpmg.com

Ireland

Paul Dobey
Tel: +353 1 410 1152
E-mail: paul.dobey@kpmg.ie

Israel

Haim Rotlevy
Tel: +972 3 684 8516
E-mail: hrotlevy@kpmg.com

Italy

Fabiano Gobbo
Tel: +39 02 67 6431
E-mail: fgobbo@kpmg.it

Japan

Roberto Esposito
Tel: +81 3 3595 7070
E-mail: roberto.esposito@jp.kpmg.com

Korea

Kyo-Tae Kim
Tel: +82 2 2112 0400
E-mail: kkim1@kr.kpmg.com

Kuwait

James Stuart
Tel: +965 242 6999
E-mail: jamesstuart@kpmg.com.kw

Latvia

Patrick Querubin
Tel: +371 703 8000
E-mail: patrick.querubin@kpmg.lv

Luxembourg

Ravi Beegun
Tel: +352 225 151 248
E-mail: ravi.beegun@kpmg.lu

Malaysia

John HH Lee
Tel: +60 3 2095 3388
E-mail: jhhlee@kpmg.com.my

Mexico/Panama

Nicolás Olea
Tel: +52 55 5246 8678
E-mail: nolea@kpmg.com

Netherlands

Jereon van Nek
Tel: +31 20 656 7360
E-mail: vannek.jereon@kpmg.nl

Norway

Christian Johansen
Tel: +47 2109 2463
E-mail: christian.johansen@kpmg.no

Philippines

Fernando Castro
Tel: +63 2 885 7000
E-mail: fcastro@kpmg.com

Poland

Bożena Graczyk
Tel: +48 22 528 1073
E-mail: bgraczyk@kpmg.pl

Portugal

Ines Viegas
Tel: +351 220 102 300
E-mail: iviegas@kpmg.com

Qatar/Bahrain

Doug Tait
Tel: +973 21 13 78
E-mail: dougtait@kpmg.com

Russia

Natalia Lukashova
Tel: +7 095 937 2503
E-mail: nlukashova@kpmg.com

Singapore

Ah Too Teng
Tel: +65 6213 1670
E-mail: ahtooteng@kpmg.com.sg

South Africa

John Martin
Tel: +27 11 647 8038
E-mail: john.martin@kpmg.co.za

Spain

Luis Martin Riaño
Tel: +34 91 4563 495
E-mail: lamartin@kpmg.es

Sweden

Per Lönnqvist
Tel: +46 8 723 6112
E-mail: per.lonnqvist@kpmg.se

Switzerland

Tapio Koch
Tel: +41 1 249 2915
E-mail: tapiokoch@kpmg.com

Taiwan

Tracy Y.I. Li
Tel: +886 2 2715 9999
E-mail: tracyli@kpmg.com.tw

Thailand

Michael Haddon
Tel: +66 2 658 5000
E-mail: mhaddon@kpmg.co.th

Turkey

Yardimci Ebru
Tel: +90 212 213 7042
E-mail: eyardimci@kpmg.com.tr

United Arab Emirates

Roy Hattingsh
Tel: +971 4 403 0323
E-mail: royhattingsh@kpmg.com

United Kingdom

Angus Grant
Tel: +44 20 7311 6040
E-mail: angus.grant@kpmg.co.uk

United States

Steven M. Roberts
Tel: +1 202 533 3018
E-mail: sroberts@kpmg.com

Steve Whiting
Tel: +1 203 406 8302
E-mail: swhiting@kpmg.com