Operational Risk Regulatory Approach Discussion Paper

September 2000

ISDA®

International Swaps and Derivatives Association, Inc

INTERNATIONAL SWAPS AND DERIVATIVES ASSOCIATION

European Office
One New Change
London EC4M 9QQ
Telephone: +44 (0)20 7330 3550
Facsimile: +44 (0)20 7330 3555

North American Office
600 Fifth Avenue, 27th Floor
Rockefeller Center
New York, NY 10020-2302
Telephone: +1 212 332 1200
Facsimile: +1 212 332 1212

Japanese Office
Chuo Building, 1st Floor
2-17 Kagurazaka
Shinjuku-ku
Tokyo 162-0825
Telephone: +81 3 5227 3282
Facsimile: +81 3 5227 3283

Website: www.isda.org
E-mail: isda@isda.org

Contents

1 Executive Summary

In the context of the past year's discussions about the regulatory treatment of operational risk, ISDA member firms decided in April 2000 to proceed with a project to identify and where possible rank those qualitative criteria that were relevant to the assessment of a firm's effectiveness in managing operational risk.

This project follows on from two earlier pieces of work: 'Operational Risk – The Next Frontier'; and ISDA's March 2000 response to the consultative papers on a new capital framework issued in 1999 by the Basel Committee on Banking Supervision and the EU Commission.

This paper seeks to bring a structured approach to the assessment of qualitative factors in operational risk management and reflects the need for an objective, internationally applicable approach to assessing operational risk.

Objective

Specifically, the project's primary objective is to: "Identify qualitative criteria that support the appraisal of operational risk management by institutions."

In doing this the following factors have been taken into account:

- The principles underpinning operational risk management practice;
- Elements of a leading practice operational risk management framework;
- What components of an institution's risk management approach are important in a qualitative assessment;
- Challenges for regulators in implementing a qualitative approach.

It is essential that any framework for managing operational risk must be integrated with the management of other forms of risk, i.e. credit and market risk. It is therefore important that the principles and guidelines for operational risk management are considered within the context of an overall framework for risk management.

Qualitative approach

The report analyses the use of qualitative criteria in relation to the four quantitative techniques outlined in the April 2000 Risk Management Group discussion paper and also in the Industry Technical Working Group paper of July 2000, by using these qualitative criteria to assess a firm's eligibility to use any of the four techniques.

Implementation of a regulatory approach

As any workable regulatory approach will have to take into account a number of regulatory considerations, this project has considered the following:

- Scalability, with regard to the differing levels of complexity of business within supervised institutions;
- Culture, given differences of legal/administrative systems and of supervisory tools;
- Consistency, achieved through a clear and transparent framework with a defined and focused set of assessment criteria;
- Resources, in terms of both the number and the type of supervisory staff that may be required;
- Balance of accuracy and practicality/cost-effectiveness;
- Incentives –any framework should encourage the optimisation of controls within financial institutions.

Further implementation issues are also discussed, including the possibilities for:

- Benchmarking
- Self-assessment
- Third-party assessment (whether by supervisors or other competent entities).

Industry practice

Guidelines as to leading practice for operational risk management in financial institutions are set out in the Appendix.

The operational risk management framework is built around an integrated, reiterating cycle of risk management with three key components:

- Organisational structure (role of board, corporate governance, operational risk function);
- Strategy and policy (strategy, policy, procedures); and
- Risk management process (identification, assessment/quantification, mitigation, monitoring and reporting).

Conclusion

This paper is seen by ISDA members as a basis for future discussion on the assessment of qualitative factors of relevance to operational risk management. It is widely recognised that the regulatory treatment of operational risk is still evolving and the current report has been drafted with that evolution in mind. At the same time, the intention has been to set out the key issues for consideration, in anticipation that these are the ones that will form the focus of future discussion. ISDA believes that it is through such discussion that the shared objective of optimised management of operational risk in financial institutions will best be achieved.

Acknowledgements

The drafting of this report was facilitated by a team from PricewaterhouseCoopers, led by Andrew Gray and Sally Williams. ISDA and PwC wish to thank the following institutions and individuals for their generous support in the current project, particularly for their invaluable advice and readiness to share their experience of the reality of managing operational risk.

ABN AMRO	Sandrijn Weites
Barclays	Adrian Belton
Bank of America	Charlene Balfour
	Tunde Pampam
Bank of Tokyo-Mitsubishi	Mark Balfan
	Frank Fronzo
BBV-Argentaria	Jordi García
BNP Paribas	Catherine Coste
	Eric Vandamme
CIBC	Tony Peccia
Chase Manhattan Bank	Aditya Mohan
Citibank	Jay Newberry
	Eugenia Singer
	Howard Stein
Credit Suisse Group	David Lau
Deutsche Bank	Mark Laycock
Dresdner Bank	Jonathan Howitt
Halifax	Ammy Seth
JP Morgan	Joseph Sabatini
Lloyds TSB	Stuart O'Nions
Merrill Lynch	David Murphy
Royal Bank of Scotland	Anita Millar
	Chris Rachlin
Standard Bank of South Africa	Dennis Everett
Société Générale	Brigitte Declercy
State Street	Mary Jane Burke
UBS	Jonathan Davies
	Mattia Rattaggi

2 Introduction

Objectives of this discussion paper

In the context of the current debate around a regulatory capital charge for other risk generated by the proposal from Basel to reform the 1988 Capital Accord[1], and from the EU Commission to reform the Capital Adequacy Directive,[2] the key objective of this discussion paper is:

To identify qualitative criteria that support the appraisal of operational risk management by institutions. These qualitative criteria should be capable of being applied to the proposed quantitative regulatory approach to calculate an operational risk capital charge.

In meeting this objective the following points are considered:

The fundamental principles that underpin operational risk management leading practice	Section 3
How such a qualitative assessment can be applied to the regulatory approach for a capital charge	Section 4
Which components of an institution's approach to operational risk are important, in a qualitative context, as a greater degree of sophistication is sought	Section 4
The extent to which any approach for calculating an operational risk capital charge should take into account factors specific to individual institutions and factors that are relevant to industry groups	Section 4
The challenges for regulators implementing an approach for calculating an operational risk capital charge	Section 5
Elements of a leading practice operational risk management framework	Appendix

In preparing this discussion paper we have also been mindful of:

- Current industry developments – within both individual institutions and industry bodies/working groups – for example, the current industry debate on business line/risk type matrices; and

- The need for an approach to calculating a capital charge that is capable of being rolled out on a wide scale and which therefore incorporates simpler methods, such as the Basic Indicator, as well as more complex methods such as Modelling, as discussed in the Risk Management Group Discussion Paper[3].

[1] *A New Capital Adequacy Framework, June 1999.*
[2] *A Review of Regulatory Capital Requirements for EU Credit Institutions and Investment Firms, November 1999, European Commission Services.*
[3] *Other Risks Discussion Paper, April 2000, Risk Management Group, Basel Committee on Banking Supervision*

The following assumptions have also been made:

- For the purposes of this paper, the definition of operational risk is based on that used in the recent ISDA/BBA/RMA survey[4], i.e.
  "*Operational risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events."*

- *The distinction between other risks and operational risk:* Operational risk, as defined above, is generally viewed as being a sub-set of Other Risks. Other Risks may also include business risks and strategic risks. The immediate focus of this discussion paper is on operational risk.

- *The relationship between risks and controls:* When management considers its exposure to operational risk, it is necessary to assess 1) what aspects of operational risk the institution is exposed to, as well as 2) how well the institution is managing this exposure to operational risk. When an institution has implemented controls to manage this exposure, the remaining residual risk is the level of risk to which the institution chooses to be exposed to in the course of its business. An institution will typically implement an operational risk management framework in order to monitor the effectiveness of these controls, the level of residual risk and their compatibility with its operational risk management objectives and policies.

- *Whilst there is a relationship between size and capital, this relationship is not linear. Furthermore, an increase in the size and/or complexity alone of an institution should not automatically result in generating a higher capital charge.* The regulatory approach set out here would enable the adequacy and quality of application of the governance, control and risk management framework, as well as the likely impact of any loss sustained, to be key factors in the calculation of a capital charge.

[4] *Operational Risk, The Next Frontier, December 1999, available from ISDA. (Various industry groups are currently involved in work on defining operational risk. The aim of this paper is not to replicate or pre-empt this work, and for this reason a definition based on the ISDA/BBA/RMA definition has been adopted here).*

3 Operational Risk Management Principles

3.1 Operational Risk Management

Risk management is the overall process by which an institution:

- Identifies and understands the full spectrum of its risks;
- Defines its appetite for risk, based on strategic objectives;
- Assesses the risks and means of mitigation on a cost/benefit basis in order to take informed actions;
- Reduces the likelihood and impact of loss events; and
- Decreases the uncertainty of overall performance.

This process is illustrated in the diagram in Appendix 1.

Operational Risk Management relates to the management of those risks that could lead to a loss resulting from inadequate or failed internal processes, people and systems, or from external events.

An operational risk management framework is a framework built around a reiterating cycle of risk management, with three key components:

- Organisational structure (including Board roles and responsibilities, corporate governance procedures and operational risk function);
- Strategy and policy (operational risk management strategy, policies and procedures);
- Operational risk management process (processes for the identification, assessment/ quantification, management/mitigation, monitoring and reporting of operational risks).

It should be noted that the underlying concepts of risk management apply to all types of risk (i.e. credit risk, market risk and operational risk). The principles and leading practice guidelines set out in this paper and its appendices focus specifically on operational risk management. However, in developing their own frameworks, institutions will inevitably need to consider how their procedures and frameworks for managing different types of risk should be integrated, in order to ensure both consistency and completeness in their overall risk management approach.

3.2 Operational Risk Management Principles

There are 6 fundamental principles that all institutions, regardless of their size or complexity, should address in their approach to operational risk management and these are set out in the table below:

Governance and establishment of the prerequisites for a risk management framework	1	**Ultimate accountability for operational risk management rests with the board**, and the level of risk that the organisation accepts, together with the basis for managing those risks, is driven from the top down by those charged with overall responsibility for running the business.
	2	**The board and executive management should ensure that there is an effective, integrated operational risk management framework**. This should incorporate a clearly defined organisational structure, with defined roles and responsibilities for all aspects of operational risk management/monitoring and appropriate tools that support the identification, assessment, control and reporting of key risks.
	3	**Board and executive management should recognise, understand and have defined all categories of operational risk applicable to the institution**. Furthermore they should ensure that their operational risk management framework adequately covers all of these categories of operational risk, including those that do not readily lend themselves to measurement.
Risk management framework fundamental requirements	4	**Operational risk policies and procedures that clearly define the way in which all aspects of operational risk are managed should be documented and communicated**. These operational risk management policies and procedures should be aligned to the overall business strategy and should support the continuous improvement of risk management.
	5	**All business and support functions should be an integral part of the overall operational risk management framework** in order to enable the institution to manage effectively the key operational risks facing the institution.
	6	**Line management should establish processes for the identification, assessment, mitigation, monitoring and reporting of operational risks** that are appropriate to the needs of the institution, easy to implement, operate consistently over time and support an organisational view of operational risks and material failures.

As these principles are consistent with those communicated by Basel,[5] and given their fundamental nature, they need to be reflected in any regulatory model for setting an operational risk capital charge. ISDA has considered how this might be achieved in section 4 below. In addition, it has included guidance on how institutions might apply these principles by developing an operational risk management framework in the Appendix. The guidelines set out in the Appendix are a statement of industry leading practice and as such reflect operational risk management practice towards which institutions should be working.

[5] *Framework for Internal Control Systems in Banking Organisations, September 1998.*

4 Proposed Qualitative Assessment

There is strong support in the industry for a regulatory capital assessment model that allows institutions managing operational risk effectively access to a more precise means of calculating an operational risk capital charge. This is consistent with the shared view of industry and regulators that institutions should benefit from more sophisticated controls and that the regulatory regime should establish incentives to improve risk management and controls.

These objectives are met by the proposed quantitative techniques once internal loss data is incorporated into the operational risk capital charge calculation, as any institution with an effective control environment would normally expect to have a lower loss experience, and thus a lower capital charge.

There is, however, significant concern that such a purely quantitative approach could enable institutions with poor operational risk management processes and controls, but with access to internal loss event data, to achieve a lower capital charge than institutions with stronger risk management processes but no access to internal loss event data.

There is also concern about the method of calculation of operational risk capital for an institution that has in the recent past experienced serious loss but where management has reacted and strengthened the control environment in that area, and consequently reduced the likelihood of recurrence, or where the probability of loss had been very low. In such a situation, a purely quantitative approach would cause an institution to carry an increased capital charge with no account taken of the improved control environment.

In order to address such issues this section seeks to identify ***qualitative*** criteria which could be integrated into the process (as currently proposed by the Industry Technical Working Group on Operational Risk[5]) for determining the regulatory capital requirement for operational risk. In doing so, the primary issue to address is *what qualitative standards can be defined as the operational risk prerequisite criteria for selecting a quantitative technique,* and we consider this in Section 4.1 below.

Furthermore, following the calculation of the quantitative element of the capital charge it is important to build in a capital incentive for further improvements in:

- The sophistication of the operational risk framework (for example, this might include where institutions are able to demonstrate that significant progress has been made towards meeting the qualitative requirements for the next quantitative technique); and
- The effectiveness of the operational risk controls in place (for example, this might include where institutions are able to demonstrate that they have reduced the actual level of risk existing within the business).

However, given the current stage of the debate about qualitative factors in relation to operational risk capital charges, this paper does not seek to address how capital charges could be adjusted where institutions are able to demonstrate either of the above.

[5] *Working Paper on Operational Risk Regulatory Capital by the Industry Technical Working Group on Operational Risk, July 2000*

4.1 Qualifying Criteria for Quantitative Techniques

The Industry Technical Group on Operational Risk has recently issued a paper defining four options to calculate a regulatory capital charge for operational risk.[6] The basis of this approach is that there are four choices for calculating the quantitative element, of increasing sophistication, providing increasing accuracy.

The less sophisticated choices (the Basic Indicator approach and the Standard Lines of Business approach) calculate charges using industry data and standardised indicators and would be defined by the regulator. The third and fourth approaches enable institutions to use their own data and more sophisticated statistical approaches, which therefore calculate charges more reflective of the institution's own operational risks.

It is likely that the more sophisticated approaches will remove the need for, or reduce the size of, the capital 'buffer' which is inevitably required in the less sophisticated approaches. As a result, there is an incentive for institutions to use the more sophisticated approaches. As institutions move to more sophisticated approaches, they will not only need more developed control structures but they will face the not inconsiderable burden of collecting high quality, detailed, accurate, and complete internal loss event data.

There is general industry consensus about the need to provide clearer parameters around the eligibility for selecting each quantitative technique, in order to provide comfort that institutions take ownership for the accurate calculation of capital charges. ISDA proposes that this could be achieved by setting minimum qualitative criteria for the use of each of the quantitative approaches. This in turn would encourage better understanding and management of risks and provide more confidence in the robustness of the quantitative technique.

Such an approach would necessitate a regulatory assessment of the level of sophistication of an institution's operational risk management processes. Once the regulator is satisfied that the criteria for the next level of sophistication have been adequately met, regulatory approval would be given for use of the related quantitative technique. (Suggestions on how this regulatory assessment might be performed are given in the next section.)

Just as an institution should be able to choose its overall approach, it should be able to apply different approaches to different business units. This presents several advantages:

- It encourages improvements to be made as they become possible – progress is not dependent on the speed of the slowest portion of the institution;
- It allows institutions to focus efforts; and
- It allows tailored solutions for individual units.

[6] *Working Paper on Operational Risk Regulatory Capital by the Industry Technical Working Group on Operational Risk, July 2000.*

Clearly, in such cases:

- The qualitative criteria for the relevant quantitative technique being adopted would be applied to the business lines individually; and
- The loss data that the institution is required to submit to the regulator should only be increased for those business lines using sophisticated techniques.

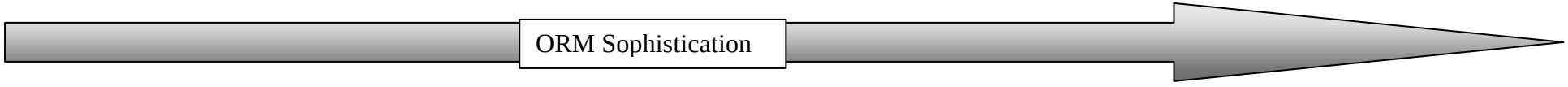
Furthermore, this should logically be used to enable institutions to focus their work on material business lines. Hence, institutions should only be required to gather loss data for their material business lines.

In the table overleaf we have set out features or "themes" that could be used to distinguish between each of the four different stages. Underlying each of these themes, we have proposed qualitative criteria based on a more granular analysis of the six fundamental risk management principles detailed in section 3. An institution must consistently demonstrate attainment of these criteria over a period of time (for example, one year as is adopted for Market Risk Models) to be allowed to use that particular quantitative technique.

Assuming satisfaction of the relevant criteria, the approach that an institution selects to calculate operational risk capital charges should be a free choice of management, subject to the requirement that it should be appropriate to the nature and complexities of the business. Hence an institution that is using the basic indicator technique should not necessarily be regarded as having inadequate operational risk management procedures.

Fig 1: Qualitative criteria for quantitative techniques

	Basic Indicator Single indicator, regulator-determined, industry data	**Standard Lines of Business** Standardised multiple indicators and business lines, regulator-determined, industry data	**Internal Risk** Institution-determined indicators, business lines and data	**Internal Models** Institution-determined models and data
	Internal control environment exists, but is not risk based	Effective risk based control framework includes risk identification and mitigation processes	Effective operational risk management framework, including aggregation of risk positions at organisational level	Measurement/modelling based on comprehensive loss data
		Demonstrates all criteria in preceding stage and:	**Demonstrates all criteria in preceding stage and:**	**Demonstrates all criteria in preceding stage and:**
Governance	Board acknowledges and owns operational risk (OR)	Risk strategy defined and identified risk appetite. Risk management tools and policies Executive Risk Management Committee approves ORM policies ORM organisational structure established ORM roles and responsibilities clearly communicated and understood at business unit level	OR function independent from risk takers Active Head of OR and OR Committee, where appropriate independent from risk takers Central co-ordination of OR across business	As for Internal Risk approach
Framework	Risk management through individual mitigation programmes Reliance on quality of people and culture	ORM framework in place including: • Defined policies for identification, assessment, management and reporting • Definition of OR, includes clear boundaries with other forms of risk • Operational risk categories clearly defined • Risk language clearly defined • Key risk indicators (KRIs) identified for OR events • Responsibilities and accountabilities in business lines clear and understood • Consistent OR practices across business	Common definition of OR incidents Definition of loss events Loss event measures put in place and linked to loss limits Formal escalation process in place for KRIs Information systems capable of supporting data collection	Collation and analysis of comprehensive data on timely basis Information systems capable of supporting data collection and model calculation Pass regulatory model recognition process
	Basic internal control environment	Risk based audit process established	Evaluation of OR mitigation efforts against risk appetite and business objectives	OR integrated into business performance measurement process
Reporting	Director OR losses reported to Board after the fact	Regular OR reports to Senior Management and Board escalating issues by outlining losses and indicators KRIs reported at business line level Critical ORs reported with exposures and plans to address action plans Considered measures to enable loss data collection	Consolidation and transparency of risk positions at group/institution level OR reports include incident reporting in terms of total consequence Report of losses and evaluation of effectiveness of mitigating actions Timely collection/collation of data for relevant business lines/loss types	Dedicated resource for Operational Risk quantification modelling Statistical quantification of operational risk charge



5 Implementation Issues

Any regulatory assessment for operational risk must both:

(a) Reflect the reality of business and be compatible with and conducive to good business practice; and
(b) Be practicable from the regulators' point of view.

The proposed qualitative assessment described in Section 4 has been developed to comply with (a) and this section considers (b).

5.1 Regulatory Implications

Any workable operational risk regulatory approach will have to take into account a number of high-level but fundamental regulatory considerations. ISDA believes the key regulatory issues are as follows:

- **Scalability** – the approach must be workable for both small and large institutions, and different levels of sophistication. Also, whilst some countries may apply the new Capital Accord to the whole of their banking and securities industry, others may well limit it to only a small sub-set:

  - ➢ The approach does not differentiate on the basis of the size of the institution, but on the sophistication of the institution.
  - ➢ It allows institutions, subject to regulatory approval, to select the quantitative technique best suited to themselves and their state of development.
  - ➢ In addition, it allows institutions to select different quantitative techniques for different business lines. This means that firms can achieve regulatory recognition for their achievements in defined business areas, even if the same state of advancement has not necessarily been attained across the whole institution. (This may be as a result of a cost-benefit analysis of increasing sophistication in different business areas.)

- **Application** – the approach must be capable of being applied in countries which have differing legal systems and business cultures, and which have differing regulatory tools at their disposal (see Methods of Implementation, below). The approach:

  - ➢ Does not presuppose the use of particular regulatory tools but is compatible with a range of supervisory practices and regimes.
  - ➢ Provides a clear and transparent mechanism in which supervisors can arrive at judgements about the state of an institution's controls over operational risk. This means that it can be adopted within a range of supervisory regimes and practices.

- ➢ Encourages the institution to "know itself" and to develop risk control practices compatible with leading practice. This is consistent with the approaches and principles outlined by the Basel Committee.[7]

- **'Level playing field'** – While the regulation of institutions is moving towards more 'bespoke' solutions (internal models being the ultimate expression of this), the approach, and the way it is implemented, must ensure to the fullest extent possible that the exercise of supervisory judgement will yield reasonably consistent results within and across jurisdictions, if it is to enjoy the confidence of national authorities and the regulated community. ISDA believes that this can be secured as:

  - ➢ The approach provides a clear and transparent way in which institutions and regulators may address operational risk, and the mechanism for determining its contribution to the capital charge.
  - ➢ While individual regulators may have their own individual mix of on and off-site supervision, the criteria for moving from one quantitative technique to the next can be applied consistently irrespective of that mix.
  - ➢ It is envisaged that the overwhelming majority of institutions would use either the basic indicator or the standard lines of business methods. The criteria for moving between these techniques in particular, while qualitative, are capable of being turned into a checklist.

- **Flexibility** – The approach is sufficiently flexible to enable implementation in the face of a number of potential resourcing issues, for example:

  - ➢ The approach recognises that there are many ways to achieve an objective. For example, while supervisors might retain the primary inspection role, nothing should prevent them making use of external sources of information or resources as appropriate.
  - ➢ Similarly, use can also be made of independent internal functions such as internal audit and inspection functions within the institution itself.[8]

- A **balance between simplicity and sophistication** – an overly engineered approach risks placing a burden on firms and regulators without a commensurate increase in supervisory benefits. At the same time the approach needs to be sufficiently sophisticated to differentiate appropriately between firms.

  - ➢ See the comments above on how the approach supports scalability.

[7] See in particular, *Framework for Internal Controls Systems in Banking Organisations (September 1988)*, and *Enhancing Corporate Governance for Banking Organisations (September 1999)*.

[8] The particular role of internal audit, and the nature of the collaboration between regulators, internal and external auditors is discussed in *Internal audit in banking organisation and the relationship of the supervisory authorities with internal and external auditors, Consultative Papers of the Basel Committee on Banking Supervision (July 2000).*

- ➢ In the same way that different regulators may use different methods or a different mix of methods to secure the same objective, different firms also need to be able to use different methods to achieve the same goal. The above approach, by focusing on outputs, allows firms the choice of means to secure those outputs.
- ➢ Firms may also elect to apply different techniques to different business lines, depending on the degree of advancement in risk control in a particular area and on a cost-benefit analysis of increasing sophistication in a given area.

- **Incentives** for good risk management – any approach needs to encourage sound risk management within firms by clearly setting out the supervisory benefits to be gained from improving the quality of their controls. The approach, similarly, needs to work with the emerging industry standards in the field of operational risk (see comments on how the approach supports scalability):

  - ➢ Institutions that choose to make investment in good risk management are rewarded by being able to use more sophisticated techniques for calculating capital requirements. This may yield some capital saving, but the real attraction is being able to use internal data and systems, and aligning regulatory and internal approaches to risk. Supervisors should welcome this development as it will allow them to discuss operational risk on the same terms as the supervised institution, rather than on the basis of regulatory measures which have no real meaning for the supervised institution. Thus good risk management and good supervision become mutually reinforcing.

5.2 Methods of implementation

Ensuring Consistency
As we identify above, it is important that the regulatory approach enables broadly consistent judgements within and across supervisory regimes. There are a number of ways in which institutions and supervisors can work together to ensure that this common objective is attained:

- Devising and using 'multiple choice' type questionnaires to narrow the range of potential outcomes;
- Supervisors developing a shared understanding through working level regulatory groups, such as that successfully used within an EU context for the implementation of VaR model recognition;
- Charting and publishing information on emerging leading practice, building on the various papers that the Basel Committee, and industry bodies, have already published on corporate governance, internal controls and risk management; and
- Collecting and sharing data on an international basis. The Basel Secretariat could play an active role in this area by, for example, using a web-site to disseminate information. Such information could include:

  - ➢ Definitions of business lines
  - ➢ Loss data
  - ➢ Developing benchmarks.

Different methodologies for assessing the operational risk management framework
The regulators could implement the approach using some or all of the following techniques, according to the mix that best suits their legal environment, culture and resourcing:

- **Self-assessment by institutions** – Institutions could complete a self-assessment process. (This could be reviewed by internal audit/external auditors/regulators, to provide assurance on completeness and accuracy of the answers, prior to the regulators defining the regulatory capital requirement.)

- **Assessment by third parties** – Basel has long recognised that external auditors in particular have a particular expertise in respect of internal controls.[9] Use of such experts could provide regulators with:

  - ➢ Confidence in the technical soundness and independence of the self-assessment review.
  - ➢ Provide on-site inspection capability in addition to, or as an alternative to self-assessment.
  - ➢ Additional resource to meet shortfalls that may occur at some regulators.

The specifics of third party assessment of risk management, as opposed to internal controls, is a separate issue that needs further debate as to the possible suitable third parties for this.

- **Assessment by regulators** - Regulators could perform the assessment themselves. In doing this, they could utilise current skills built up in conducting on-site examinations, performing model reviews and other elements of risk-based supervision, for example RATE in the UK, or CAMEL in the USA.

It may be that regulators wish to use a combination of the above methods. For example, there might be little on-site inspection for an institution using the basic indictor technique, but for an institution moving to a more complex technique, the regulator may wish to use both their own resources and those of an expert third party. However, as the regulator develops confidence in a particular institution's operational risk management framework, the regulator may find it satisfactory to rely on internal assessments supplemented by internal and external audit reports as necessary. As the Basel Committee itself has noted "co-operation between the supervisor, the internal and external auditor optimises supervision".[10]

[9] *The Relationship between Bank Supervisors and External Auditors (a joint paper issued as an International Statement on Auditing by the International Auditing Practices Committee), Basel Committee on Banking Supervision (July 1989).*
[10] *Internal audit in banking organisations and the relationship of the supervisory authorities with internal and external auditors, Consultative Paper of the Basel Committee on Banking Supervision, July 2000.*

Appendix Operational Risk Management Framework Leading practice guidelines

Operational Risk Management Framework

This section outlines the key components of operational risk management. Its purpose is to articulate leading practice in operational risk management. It should be noted that operational risk management is a fast developing practice, and the guidance set out in this document is limited to practice at the current time.

In developing an operational risk management framework institutions will inevitably need to consider how their procedures and frameworks for managing different types of risk (i.e. credit, market and operational risks) should be integrated, in order to ensure both consistency and completeness in their overall risk management approach. The operational risk management framework should therefore be developed within the parameters of, or to interface with, the institution's existing risk management organisation, policies and practices.

In order to address operational risk in an efficient and effective manner, management should first establish the context for operational risk management within the institution, via an operational risk management framework, and then develop and implement day-to-day procedures for applying that framework.

We have set out below an outline of the principal topics that senior management would normally expect to consider in developing an efficient and effective operational risk management framework. Our objective here is to provide guidance on current leading practice, and this section should not, therefore, be regarded as a prescriptive approach for managing operational risk.

An operational risk management framework would normally encompass the dimensions set out in the diagram below:

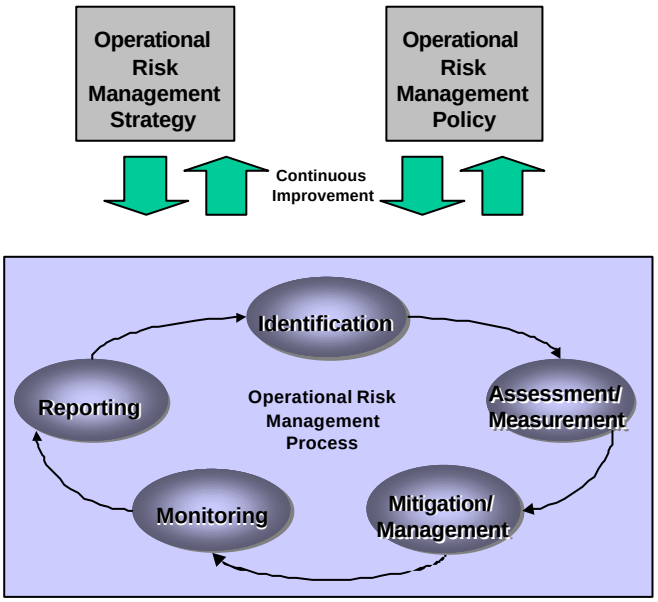


Fig 2: Operational Risk Management Framework

Each of these aspects are considered in more detail below.

Risk Management Organisational Structure

In order to ensure that operational risk management activities are clearly understood and executed, management should define an organisational structure for operational risk management and communicate individual roles and responsibilities. Whilst ultimate responsibility for operational risk management resides with the Board, it is essential that:

- Every member of the institution clearly understands their individual role in the risk management process; and
- A risk-aware environment and culture be created, which supports the identification and escalation of operational risk-related issues.

Role of the Board of Directors

Responsibility for operational risk management ultimately rests with the Board, or its equivalent. Although the Board may delegate the management of this process, it must ensure that its requirements are being executed. This responsibility requires directors to have a thorough understanding of the institution's full spectrum of products, processes and associated risks.

Good practice suggests that:

- There should be an individual director who is responsible for operational risk and is independent from the risk takers;
- The Board may also establish a committee (or other appropriate mechanism) to authorise and manage day-to-day decisions for implementing the institution's operational risk strategy and for ensuring that there are processes in place to manage and escalate operational risk issues from all sources within the institution; and
- The Board should review operational risk reports on a regular basis in order to ensure that its requirements for operational risk management are being met.

Corporate Governance

Corporate Governance is the general term used to describe the manner in which the business and affairs of an institution are governed by their board of directors and senior management. This includes how an institution:

- Sets (establishes and communicates) corporate objectives;
- Oversees the day to day operations of the business;
- Considers the interests of stakeholders;
- Aligns corporate activities and behaviour with the expectation that the institution will act in a safe and sound manner and in compliance with applicable laws and regulations; and
- Protects the interests of depositors, customers and other interested parties.

The Basel Committee has identified a number of practices as critical elements of any corporate governance process and these should be accommodated within the operational risk management framework.[11]

Operational Risk Function

An operational risk management function should be established in a similar manner to institutional credit and market risk functions and interface with those by reporting to the central risk function. As such the operational risk function should be independent of internal audit.

The role of the operational risk management function is to work with management to assist them in meeting their responsibility for understanding and managing operational risks by:

- Assessing, monitoring and reporting operational risks for the institution as a whole; and
- Assessing whether risk management practices have been carried out in accordance with operational risk strategy and policies.

In so doing it performs a number of roles:

- Establishment of specific policies and standards
- Co-ordination of risk management activities
- Initial structured risk assessment
- Monitoring & Incident handling
- Status reporting to Executive Management and Director
- Identification of relevant support tools and guidance
- Liaison with Internal and External Audit

Operational Risk Management Strategy and Policy

Operational Risk Management Strategy

In order to put in place an effective operational risk management framework, an institution needs to identify its stakeholders, and understand their requirements and its obligations to them. This facilitates the identification of key business drivers and objectives that are relevant when determining the institution's operational risk management strategy.

Once these objectives are known, the institution should consider the strategic challenges it faces in delivering those objectives and the consequences of not doing so, and thereby establish an operational risk management strategy. Based on these objectives, the institution can design and implement an operational risk framework to identify, understand and manage operational risk, which fully meets its requirements.

Responsibility for defining the operational risk management strategy, and for ensuring it is aligned with overall business objectives, should rest with the Board.

[11] *Enhancing Corporate Governance for Banking Organisations, Basel Committee on Banking Supervision (September 1999)*

Operational Risk Management Policy

An institution's approach to operational risk management should be embedded within policies, which set out operational risk management standards and objectives for all key underlying business and support processes.

These policies should:

- be designed to govern risk management in all business activities;
- facilitate the monitoring, measurement and management of such activities;
- reflect the internal and external environment within which the business activities take place; and
- be subject to regular review and update.

Operational risk policies should consider:

- *Strategy*: Whether the appetite for operational risk is consistent with the strategic objectives of the institution;
- *Scope and application*: Defining the areas covered by the policy; and
- *Resourcing*: The Board, sub-committee and personnel responsible for various facets of operational risk management.

Operational risk management policies should create the mechanisms by which an institution can identify, measure and monitor all significant operational risks, indicating the tools to be used to measure each category of risk, and as such should be:

- Approved by the Board;
- Appropriate to the scale of risk and activity undertaken;
- Fully understood by the people responsible for managing these risks;
- Clearly communicated to all employees within the institution on a regular basis, to ensure that awareness levels are maintained and that they are consistently applied; and
- Subject to regular review and update, in order to ensure they continue to reflect the environment within which the institution operates.

Areas that operational risk management polices might cover include:

- New Product Development
- Internal Control
- Information Technology
- Change Management
- Human Resources
- Business Continuity Planning
- Internal Audit

Operational Risk Management Procedures

Once operational risk management policies have been established by an institution, adequate procedures should be designed and implemented by the business lines, to ensure compliance with these policies at business line level.

Operational Risk Management Processes

In order to meet the above requirements of the directors and the operational risk function, policies should be implemented which encompass the following key processes:

Risk Identification

An operational risk identification and evaluation process should be established that focuses both on ***current*** and ***future*** potential operational risks.

When identifying operational risks, management should be careful to address the full spectrum of potential operational risks.

The operational risk identification process should consider:

- The full spectrum of potential operational risks;
- The internal and external environment in which the institution operates;
- The institution's strategic objectives;
- The products and services the institution provides;
- Its unique circumstances; and
- Internal and external change, and the pace of that change.

In considering operational risks, the full array of potential causes should be considered. These will include but may not be limited to:

- Transaction Processing
- Sales Practices
- Management Processes
- Human Resources
- Vendors and Suppliers
- Technology
- External Environment
- Disasters
- Unauthorised/Criminal Activities

Risk Assessment and Quantification

Once identified, operational risks should be evaluated to determine which are of an unacceptable nature and should be targeted for mitigation. This is most commonly accomplished by considering an:

- Estimate of the probability that the risk will materialise, namely the likelihood, by considering the drivers or causes of the risk; together with;
- Assessment of its impact, before taking account of the application of control strategies. The potential impact should be assessed not merely in direct financial terms but more broadly by reference to the potential effect on the realisation of corporate objectives.

As an institution aims to become more sophisticated in quantifying operational risks, complete and accurate data on operational loss events (by categories of risk) and potential sources of operational loss must be collected. The institution may then select or develop a model to fit the quantification for each category of risk.

The results of the risk assessment and quantification process will enable management to:

- Compare the risks with its operational risk strategy and policies;
- Identify those risk exposures that are unacceptable to the institution, or outside the institution's risk appetite; and
- Select and prioritise appropriate mechanisms for mitigation.

Risk Management and Mitigation of Risks

Management need to evaluate the adequacy of countermeasures, both in terms of their effectiveness in reducing the probability of a given operational risk, and of their effectiveness in reducing the impact should it occur. Where necessary, steps should be taken to design and implement cost-effective solutions to reduce the operational risk to an acceptable level. It is essential that ownership for these actions be assigned to ensure that they are instigated.

Risk management and internal control procedures should be established by the business units, though guidance from the risk function may be required, to address operational risks. While the extent and nature of the controls adopted by each institution will be different, the following areas should be considered and where appropriate, controls implemented:

- External Responsibilities (e.g. external regulatory, legal or other requirements)
- Change management
- New Counterparties and Customers
- Internal Controls
- Segregation of Duties
- Reconciliations
- IT Systems Management
- Third Party Dependencies/Shared Services
- Professional Expertise and Human Resources

- Business Continuity Planning
- Role of Internal Audit and of the risk management function itself
- Insurance.

Risk Monitoring

Senior Management should establish a programme to:

- Monitor both the qualitative and quantitative assessment of the exposure to all types of operational risk faced by the institution;
- Assess the quality and appropriateness of mitigating actions, including the extent to which identifiable risks can be transferred outside the institution; and
- Ensure that adequate controls and systems are in place to identify and address problems before they become major concerns.

It is essential that:

- Responsibility for the monitoring and controlling of operational risk should follow the same type of organisational structure that has been adopted for other risks, including market and credit risk;
- Senior Management ensure that an agreed definition of operational risk together with a mechanism for monitoring, assessing and reporting it is designed and implemented; and
- This mechanism should be appropriate to the scale of risk and activity undertaken.

Operational risk metrics or "Key Risk Indicators" (KRIs) should be established for operational risks to ensure the escalation of significant risk issues to appropriate management levels. KRIs are most easily established during the risk assessment phase. Regular reviews should be carried out by internal audit, or other qualified parties, to analyse the control environment and test the effectiveness of implemented controls, thereby ensuring business operations are conducted in a controlled manner.

Risk Reporting

Management should ensure that information is received by the appropriate people, on a timely basis, in a form and format that will aid in the monitoring and control of the business. The reporting process should include information such as:

- The critical operational risks facing, or potentially facing, the institution;
- Risk events and issues together with intended remedial actions;
- The effectiveness of actions taken;
- Details of plans taken to address any exposures where appropriate;
- Areas of stress where crystallisation of operational risks is imminent; and
- The status of steps taken to address operational risk.

The information provided should be sufficient to allow:

- Board and Executives to determine that the delegation of risk management duties has been effective and their requirements for operational risk management are being met;
- The overall risk profile to be evaluated against the institution's risk strategy and appetite;
- Key Risk Indicators to be monitored and the need for action assessed; and
- Business Unit management to confirm that controls over key risks have been executed successfully and failures/'near misses' have been escalated.

Reiteration of the Risk Management Process*:*

The risk management process outlined above (and summarised in the diagram) is an iterative process. The risk management function should ensure key operational risk management activities are revisited with appropriate frequency, e.g. annually or semi-annually

Such activities would include, but may not be limited to, determining the following:

- Operational risk strategy and policy are still aligned with the business objectives;
- Risks identified and accountabilities remain current;
- Mitigation responses remain appropriate to the operational risk strategy and policy and are still valid based on a cost benefit analysis;
- Lessons are learned from root-cause analysis and that these generate actions to improve the risk management process; and
- All actions arising are followed up in appropriate priority.

As noted above, the guidance set out in this appendix reflects leading practice at the current time.