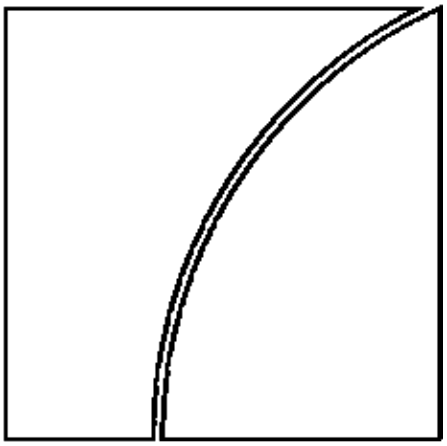
Basel Committee
on Banking Supervision



Observed range of practice in key elements of Advanced Measurement Approaches (AMA)

October 2006

BANK FOR INTERNATIONAL SETTLEMENTS

Requests for copies of publications, or for additions/changes to the mailing list, should be sent to:

Bank for International Settlements
Press & Communications
CH-4002 Basel, Switzerland

E-mail: publications@bis.org
Fax: +41 61 280 9100 and +41 61 280 8100

© *Bank for International Settlements 2005. All rights reserved. Brief excerpts may be reproduced or translated provided the source is stated.*

ISBN print: 92-9131-723-3
ISBN web: 92-9197-723-3

Contents

Observed range of practice in key elements of Advanced Measurement Approaches (AMA)

I. Background

The work of the Accord Implementation Group's Operational Risk Subgroup (AIGOR) focuses on the practical challenges associated with the development, implementation and maintenance of an operational risk management framework meeting the requirements of Basel II[1], particularly as they relate to the Advanced Measurement Approaches (AMA). The AIGOR has been specifically mandated to, among other things, exchange and catalogue subgroup members' views on operational risk implementation issues and the range of acceptable bank practices for measuring and managing operational risk under the AMA.

In recognition of the evolutionary nature of operational risk management as a risk management discipline, the Basel II Framework intentionally provides a significant degree of flexibility for banks in the development of an operational risk management framework under the AMA. It is not surprising, therefore, that the range of practice that has emerged in relation to any given issue tends to be quite broad.

The flexibility provided banks in the development of an AMA, however, should not be interpreted to suggest a lesser standard of supervisory review and assessment or that supervisors are prepared to accept as reasonable any and all responses to the challenges banks face in this area. On the contrary, prudential supervisors have an interest in identifying and encouraging bank operational risk practices that are consistent with safety and soundness and level playing field objectives. Furthermore, at various times the industry has encouraged the AIG and its subgroups to establish and maintain high standards for what constitutes acceptable practice and to publish 'sound practice' papers to communicate those standards and promote consistency across jurisdictions.

II. Purpose

Against this backdrop, the AIGOR has prepared a 'range of practice' paper using information obtained from members' supervisory work, benchmarking exercises, discussions with bank management and other sources. This paper describes specific practices that have been observed in relation to some of the key challenges AMA banks[2] currently are facing in their operational risk-related work in three subject areas: internal governance, data and modelling.[3]

---

1 'Basel II Framework' and 'Basel II', used interchangeably in this paper, refer to the Basel Committee paper *International Convergence of Capital Measurement and Capital Standards: A Revised Framework (November 2005)*.

2 'AMA bank' refers to a bank that is targeting the AMA approach in its implementation of Basel II.

3 Some of the challenges and corresponding practices covered in this paper may also be relevant to banks implementing the Standardized Approach (TSA) and, to a lesser extent, the Basic Indicator Approach (BIA). Guidance from the Basel Committee for TSA and BIA banks includes the relevant sections of Basel II and *Sound Practices for the Management and Supervision of Operational Risk (February 2003)*, which is also applicable to AMA banks.

While this paper does not address all issues or reference every practice identified with respect to any given issue, it does focus on the key issues in each of the three subject areas and provide a reasonable cross-section of the practices observed with respect to those issues. Because it is focused on bank, and not supervisory, practice, the paper does not address home-host issues.

No judgment is intended or implied regarding the acceptability of any of the practices reflected in this paper. For example, the fact that a particular practice is discussed should not be interpreted as an endorsement of that practice by the AIGOR or any of its members. Nor should the absence of a particular practice be interpreted to imply either that it is or is not considered acceptable by supervisors. The principal purpose of the paper is to catalogue the key issues and corresponding practices observed among AMA banks operating in AIGOR member countries. As such, the paper provides the international community of bank supervisors a means of framing the discussion of acceptable practice in both the management and measurement of operational risk and monitoring the evolution of industry practice and supervisors' reactions. It is also expected to be a valuable resource for both banks and national supervisors to use in their respective implementation processes.

In light of its broad membership and exposure to AMA banks, the AIGOR is an ideal forum in which the supervisory community might develop a perspective on the acceptable range of practice. In so doing, the AIGOR can facilitate greater consistency in the assessment of AMA practices among national supervisors. While the paper does not purport to define best practice, it is reasonable to expect that some of the practices identified in the development of this paper might be viewed as falling outside the range of what supervisors consider acceptable. Where observed practices are determined to be unacceptable, the AIGOR anticipates that it will identify them as such, as and when a clear consensus emerges, contributing to a narrowing of the range of practice over time. It is reasonable to expect that when a particular practice is identified as being unacceptable, national supervisors will give due consideration to the need for appropriate transitional arrangements.

This paper does not constitute new rules or revisions to the Basel II Framework. The AIGOR may update this paper from time to time as new issues are identified, industry practices evolve and supervisory experience grows.

III. Introduction

The challenges and corresponding practices identified to date have been grouped in this paper under the following subject areas: internal governance issues, data issues and modelling/quantification issues. Each subject area and the individual issues covered under them are defined. Relevant references to the Basel II Framework are included, along with a brief discussion of the significance of and challenges raised by individual issues. Finally, the observed practices are described.

IV. Internal governance issues

Definition / scope

Through various documents and other initiatives, the Basel Committee has actively promoted the adoption and implementation of sound corporate governance practices by banks and the assessment of those practices by supervisors.[4] The aim of this section of the 'range of practice' paper is not to restate existing guidance but rather to distil the key internal governance issues and corresponding practices in the management of operational risk.[5]

While the management of operational risk has always been a fundamental element of banks' risk management programmes, Basel II introduced a new dimension in the form of separate capital requirements and heightened expectations for the management of operational risk. Improvements in the internal governance and other aspects of a bank's risk management and measurement framework are expected to coincide with the increased focus on operational risk.

Internal governance issues related to the management of operational risk are not unlike those encountered in the management of credit or market risk. However, because of the more pervasive nature of operational risk and the relatively recent evolution of operational risk management as a distinct discipline, appropriate management responses to operational risk may differ in certain respects from those in other risk areas. In this context, this paper addresses the following key internal governance issues:

- the roles and responsibilities of the board of directors and senior management;
- the establishment of an independent operational risk management function;
- the day-to-day responsibilities of business line management; and,
- the responsibilities of the independent challenge function.

Specific topics and corresponding practices

i. Board and senior management involvement and understanding

The specific requirements and obligations of boards of directors and senior management are established in national legislation, regulation or codes. However, under widely accepted corporate governance principles for banks, the responsibilities of the two groups can be broadly summarised as follows:

- a board of directors is ultimately responsible for the operations and financial soundness of the bank. In partial fulfilment of that responsibility, a board of directors approves the overall business strategy of the bank, which includes the approval of the overall risk policy and risk management procedures;
- senior management is responsible for overseeing the day-to-day management of the bank.

---

[4] These efforts were evidenced most recently by the publication of the paper *Enhancing corporate governance for banking organisations (February 2006)*.

[5] Business continuity and information technology issues are not explicitly addressed in this paper. The AIGOR nonetheless acknowledges their significance in any comprehensive framework of systems and controls.

With respect to operational risk specifically, the board and senior management are responsible for overseeing the development and maintenance of a framework to effectively manage operational risk within the bank. In fact, strong board and management oversight forms the cornerstone of an effective operational risk management process.

Basel text

"In order to qualify for use of the AMA a bank must satisfy its supervisor that, at a minimum … [i]ts board of directors and senior management, as appropriate, are actively involved in the oversight of the operational risk management framework …." (paragraph 664)

"The bank's internal operational risk measurement system must be closely integrated into the day-to-day risk management processes of the bank. Its output must be an integral part of the process of monitoring and controlling the bank's operational risk profile. For instance, this information must play a prominent role in risk reporting, management reporting, internal capital allocation, and risk analysis. The bank must have techniques for allocating operational risk capital to major business lines and for creating incentives to improve the management of operational risk throughout the firm." (paragraph 666(b))

"There must be regular reporting of operational risk exposures and loss experience to business unit management, senior management, and to the board of directors. The bank must have procedures for taking appropriate action according to the information within the management reports." (paragraph 666(c))

"The bank's operational risk management system must be well documented. The bank must have a routine in place for ensuring compliance with a documented set of internal policies, controls and procedures concerning the operational risk management system, which must include policies for the treatment of non-compliance issues." (paragraph 666(d))

Issues/background

The core responsibility of, and most significant issue for, the board and senior management in this area is found in paragraph 664 of the Basel II Framework – active involvement in the oversight of the operational risk management framework. While acknowledging this responsibility, banks are seeking clarification on what constitutes 'active involvement' and how to demonstrate compliance with this requirement. There is also some uncertainty about the standard that will apply to the board and senior management of a subsidiary of an AMA bank, whether that subsidiary implements a full AMA, the hybrid approach or some other method for determining its stand-alone operational risk capital requirement.[6]

Internal governance structures for operational risk are evolving rapidly in the industry due to the relatively early stage of development of operational risk management as a distinct risk management discipline. At this critical stage, the failure of a bank's board and senior management to embrace and become engaged in a comprehensive approach to the management of operational risk may lead to the adoption of an overly narrow, compliance-

[6] Basel II and related papers make clear supervisors' expectation that the local board and management of a subsidiary bank understand the subsidiary's approach to managing and measuring operational risk. This expectation holds whether or not the subsidiary leverages the resources (management or technical) of the parent bank in the implementation of its chosen approach. Further elaboration of this concept in an operational risk context can be found in *Principles for the home-host recognition of AMA operational risk capital (Jan 2004)* and in Appendix III to the Basel Committee's press release of 11 May 2004. This concept is also discussed in general terms in *Home-host information sharing for effective Basel II implementation (June 2006)*.

oriented approach, rather than a holistic risk-oriented approach. Compliance-oriented approaches tend to be less effective in managing a bank's exposure to risk. At the same time, however, it is recognised that boards should avoid duplicating senior management's responsibilities in their efforts to provide oversight that goes beyond a compliance orientation.

Basel II and related corporate governance guidance would have the board clearly define its authority and key responsibilities, as well as those of senior management. Failure to do so could result in gaps in oversight that could potentially lead to losses, or unnecessary duplication of oversight responsibilities. As provided in paragraphs 666(c) and (d), the board of directors is responsible for overseeing management's actions and ensuring compliance with board policies as part of the checks and balances embodied in sound internal governance. Senior management is responsible for delegating duties to staff and establishing a management structure that promotes accountability, although senior management retains the ultimate responsibility to the board for the performance of the bank. Assessment of the level of involvement and understanding of the board and senior management is a critical area of ongoing supervisory focus.

The Basel II Framework also requires that the operational risk framework closely integrate the operational risk measurement system into the bank's day-to-day risk management processes – the so-called 'use test'. Under paragraph 666(b), the output of the operational risk measurement system must be an integral part of the process that the board and senior management use to monitor and control the bank's operational risk profile. This paragraph also requires that the operational risk framework incorporate techniques for the allocation of operational risk capital to major business lines and that it create incentives to improve the management of operational risk throughout the firm. The principal issues with respect to this use test requirement are the breadth of the requirement and how banks demonstrate to supervisors that the framework is actually used in the business and has not been established purely for regulatory purposes.

Range of practice

The level of involvement of boards of directors and senior management in the oversight of operational risk management frameworks varies widely among banks. In some, operational risk management concepts have been actively embraced in the belief that they may bring tangible benefits to the bank, both in terms of improved risk management and enhanced profit potential. In others, the efforts of boards and senior management appear designed solely to meet the minimum requirements of Basel II. It is important to acknowledge, however, that due to the relative immaturity of operational risk as a risk management discipline, many banks do not yet have in place fully articulated AMA models. For such banks, estimates of operational risk exposures and other critical elements of an effective operational risk framework are not yet available for board discussion.

In many banks, the board of directors has delegated oversight responsibility for operational risk management to a subcommittee. While senior management is responsible for ensuring that risk is managed appropriately throughout the bank, many banks assign significant responsibility to business units to manage the operational risk within those units.

Current efforts by banks to demonstrate 'active involvement' by boards and senior management in the oversight of the operational risk management function take many forms. In this regard, many banks have undertaken the following actions:

- development and communication of comprehensive, board-approved policies outlining all aspects of the bank's AMA framework, with the allocation of sufficient staff resources to effectively implement the policy;

- annual review by the full board of directors of the effectiveness of the AMA framework; and,
- development and implementation of comprehensive management reporting programmes through which the board and senior management regularly receive information on operational risk exposures from business units, the operational risk management function, and internal audit.

In the case of subsidiary banks, supervisors have found that there are different levels of board and senior management understanding of the subsidiary's operational risks and controls. In some cases, the local governing body and/or management do not have a deep understanding of the relevant internal governance function at the parent bank.

ii. Organisational structure – independence of the operational risk management function

The independence of the operational risk management function is an important aspect of the relationship between this function and the business lines and the areas within the bank that are responsible for assessing the effectiveness of the operational risk management framework.

Basel text

"The bank must have an independent operational risk management function that is responsible for the design and implementation of the bank's operational risk management framework. The operational risk management function is responsible for codifying firm-level policies and procedures concerning operational risk management and controls; for the design and implementation of the firm's operational risk measurement methodology; for the design and implementation of a risk-reporting system for operational risk; and for developing strategies to identify, measure, monitor and control/mitigate operational risk." (paragraph 666(a))

Issues/background

As in other areas of risk management, there is a critical need for the operational risk management function to be independent of the line function. A lack of independence in this area could result in operational risk managers becoming closely associated with the ownership of risks within a bank's business units. This will substantially reduce the function's ability to exercise professional judgement, make impartial recommendations and implement an effective framework for identifying, managing and monitoring operational risk. At the same time, however, the operational risk management function should not be so detached from the business units that it affects their familiarity with the operational risk profile and control structure of the units or their ability to quickly remediate problems as they arise. The key is striking an appropriate balance between these competing objectives.

There is no single 'right' governance model for the operational risk management function. Nevertheless, the organisational structure adopted by a bank may be an important determinant of the bank's ability to demonstrate the independence of its operational risk management function. Where circumstances exist with the potential to compromise the independence of the function, for example where a bank's operational risk management personnel also report to line management, banks will need to consider whether incremental measures should be taken to minimise this potential. Where resource constraints within a bank result in a senior operational risk manager assuming other senior management roles, supervisors should be aware of the potential for the independence of the function to be compromised or its integrity to be impaired.

Range of practice

Most banks have an operational risk management function, structurally separate from risk-generating business units, that is responsible for the design and implementation of the operational risk framework. In general, there are formal reporting lines and close cooperation between the operational risk management function and the business units. In some banks the operational risk management function has direct access to the audit committee of the board whereas in others its access is indirect (eg through the Chief Risk Officer). In some banks, staff with operational risk management or oversight responsibilities but with a dual reporting relationship to both the operational risk management function and business line management are 'embedded' in the business lines. The operational risk management function in most banks does not have other responsibilities.

Many banks point to one or more of the following indicators to demonstrate the independence of the operational risk management function:

- *Absence of improper influence*: The relationship with business units is such that opportunities for them to improperly influence the operational risk management function are minimised;
- *Head of operational risk*: An executive or senior manager is appointed with overall responsibility for the firm's operational risk management function.
- *Absence of self-interest*: The remuneration package for personnel in the operational risk management function does not depend on the operational risk performance of the business units;
- *Status*: The operational risk management function has a formal status within the bank which gives it standing, authority and independence consistent with other risk management functions;
- *Access to the audit committee*: The operational risk management function has access to the audit committee, either directly or through the same channels available to other risk management functions.

In most banks, a head of operational risk management has been appointed with responsibility for an operational risk management function with formal status within the organisation. In addition, in most banks the operational risk management function collects loss data and risk incident data from the business units and prepares regular reports for senior management and the board. In some banks the operational risk management function also collects key risk indicators from the business units.

iii. Independent internal / external challenge

Basel II requires an independent assessment by internal and/or external parties of the operational risk management and measurement framework, including AMA models. This challenge covers the activities of business units and the operational risk management function and plays a central role in both validating the operational risk management framework and ensuring data integrity and comprehensiveness.

Basel text

"Internal and/or external auditors must perform regular reviews of the operational risk management processes and measurement systems. This review must include both the activities of the business units and of the independent operational risk management function." (paragraph 666(e))

"The validation of the operational risk measurement system by external auditors and/or supervisory authorities must include the following:

- verifying that the internal validation processes are operating in a satisfactory manner; and
- making sure that data flows and processes associated with the risk measurement system are transparent and accessible. In particular, it is necessary that auditors and supervisory authorities are in a position to have easy access, whenever they judge it necessary and under appropriate procedures, to the system's specifications and parameters." (paragraph 666(f))

"The Committee recognises that the AMA soundness standard provides significant flexibility to banks in the development of an operational risk measurement and management system. However, in the development of these systems, banks must have and maintain rigorous procedures for operational risk model development and independent model validation …." (paragraph 668)

Issues/background

The challenge process within an AMA bank has two main components: the review of the operational risk management process, including related data systems, and the validation of AMA models. While these activities are distinct, they share one critical element – the need for independence in the assessment process. Independence in this context can be assessed using indicators like those referenced in the previous section. The existence of an independent challenge process is seen as central to the establishment of an effective operational risk management framework.

As it relates to the review of the operational risk management process, the challenge process falls within the traditional boundaries of internal and/or external audit responsibilities. Reviews should be sufficiently broad and detailed to permit appropriate auditor attestations regarding the activities of the business units and the independent operational risk management function, as well as the functioning of and controls within relevant operational risk data systems. However, questions may arise about whether audit staff have the expertise and familiarity with the operational risk management function to capably engage in the challenge process. If, to compensate, operational risk experts accompany audit personnel, senior management must ensure that the challenge is sufficiently independent from the operational risk management function whose work is under review.

Validation of AMA models is proving to be even more of an issue for banks. The paucity of operational loss data and the early stage of development of AMA models make it particularly difficult to address this challenge process. The availability of skilled staff may also be an issue, as it is important that banks' AMA models be adequately validated by suitably qualified parties independent of the development process to ensure they are conceptually sound and adequately capture all material risks. While model validation is often outside the scope of audit responsibilities, the audit function should ensure that AMA model validation processes are sufficiently independent and consistent with established bank policies. A related issue is the meaning of the terms 'validate' and 'verify' in their various contexts and the practical implications that arise for both banks and supervisors.

Range of practice

It is still too early to describe a 'range of practice' among banks for validating AMA models. In light of the significant staffing issues reported by many banks in this area, many are currently relying on external parties or have developed temporary internal solutions for use until they

can appropriately staff internal units capable of conducting effective testing and verification. This will be an area of increasing focus for banks and supervisors.

Practices supervisors have observed that could contribute to an effective challenge programme include:

- *Validation of data inputs, methodology and outputs*:
  a. the validation of data inputs covering all data types, including observed/actual data, constructed data, figures generated by scenario analysis and business environment and internal control factors. In the case of constructed data, the validation process ensures that any underlying assumptions are unbiased and that the results are reasonable;
  b. robust processes for developing scenarios that incorporate inputs from experienced business line managers and risk management experts. Scenarios are reviewed by an independent party and re-assessed over time by comparing them with actual loss experience (see Modelling/quantification issues);
  c. the validation of the AMA methodology. A number of banks are developing policies and procedures to ensure that model validation efforts are consistent with board and senior management expectations. These policies and procedures should be sufficiently comprehensive to address the critical elements of the validation process, including: independent review; clearly defined responsibilities for model development and validation; model documentation; validation procedures and frequency; and audit oversight. Moreover, validation activities should confirm that the relationship between the inputs and outputs of the model is stable and realistic and that the techniques underlying the model are transparent and justifiable. The model should be logical; if controls are improved, there should be a corresponding reduction in regulatory capital, all else remaining equal. This is an area that requires additional focus by banks and supervisors;
  d. processes aimed at ensuring the reasonableness of model outputs, including regulatory capital numbers, on an ongoing basis;
- *Verification of risk management processes*: A variety of techniques are being used, including steps to verify that risk management documentation is complete, management information reporting procedures are followed, captured loss data meet the relevant data standards, follow-up actions are carried out in an effective and timely manner, and procedures to review and update the operational risk management framework are followed;
- *Stress testing*: Stress testing is one of the tools commonly used to enhance and validate models. The aim of the stress test is to observe how the model would behave under unusual circumstances or in the event that key assumptions in the model break down. In the context of operational risk, however, stress testing has a narrower focus, as the capital figure, which is derived from the combination of four elements with different weights, already encompasses some types of stress test (eg the use of external data or scenario analysis to capture potentially severe tail events); and,
- *Use test*: The use test is capable of becoming one of the most effective tools in any challenge programme, often providing clear evidence to supervisors that a bank is using the relevant inputs and outputs of its AMA methodology in the day-to-day management of operational risk, as appropriate. This includes using these data to create incentives to improve risk management. Relative to the internal-ratings based approach to credit risk, however, it is generally acknowledged that the AMA

presents more of a challenge in this area because of the early stage of AMA model development.

iv. Business environment and internal control factors (BEICFs)

BEICFs are indicators of a bank's operational risk profile that reflect underlying business risk factors and an assessment of the effectiveness of the internal control environment. They introduce a forward-looking element to an AMA by considering, for example, rate of growth, new product introductions, findings from the challenge process (eg internal audit results), employee turnover and system downtime. Incorporating BEICFs into an AMA helps to ensure that key drivers of operational risk are captured and that a bank's operational risk capital estimates are sensitive to its changing operational risk profile.

Basel text

"In addition to using loss data, whether actual or scenario-based, a bank's firm-wide risk assessment methodology must capture key business environment and internal control factors that can change its operational risk profile. These factors will make a bank's risk assessment more forward-looking, more directly reflect the quality of the bank's control and operating environments, help align capital assessments with risk management objectives, and recognise both improvements and deterioration in operational risk profiles in a more immediate fashion. To qualify for regulatory capital purposes, the use of these factors in a bank's risk measurement framework must meet the following standards:

- the choice of each factor needs to be justified as a meaningful driver of risk, based on experience and involving the expert judgement of the affected business areas. Whenever possible, the factors should be translatable into quantitative measures that lend themselves to verification.
- the sensitivity of a bank's risk estimates to changes in factors and the relative weighting of the various factors need to be well reasoned. In addition to capturing changes in risk due to improvements in risk controls, the framework must also capture potential increases in risk due to greater complexity of activities or increased business volume.
- the framework and each instance of its application, including the supporting rationale for any adjustments to empirical estimates, must be documented and subject to independent review within the bank and by supervisors.
- over time, the process and the outcomes need to be validated through comparison to actual internal loss experience, relevant external data and appropriate adjustments made." (paragraph 676)

Issues/background

In principle, a bank with strong internal controls in a stable business environment will have, all else being equal, less exposure to operational risk than a bank with internal control weaknesses or that is experiencing rapid growth or introducing new products. Accordingly, banks are expected to assess the level of and trends in the operational risk and related control structures across the organisation and build the results of such assessments, generally referred to as BEICFs, into the risk management and measurement aspects of their AMA methodology. The assessments should be current and comprehensive and should identify the critical operational risks facing the bank. The assessment process should be sufficiently flexible to encompass a bank's full range of activities (including new activities), changes in internal control systems or an increased volume of information. The challenges in this area include determining which BEICFs to consider and how to build them into the model.

As the results of the risk assessment are to be incorporated in a bank's capital calculation, management must ensure that the risk assessment process is appropriate and that the results reasonably reflect the risks of the bank. For example, if a bank reduces its operational risk estimate on the strength of robust internal control factors, then there should be some process for ensuring that the impact of internal control factors on the final capital estimate is plausible, prudent and consistent with actual experience.

Range of practice

Banks have tended to focus much less on this AMA element than on the collection of internal loss data or the development of scenarios. In general, while banks have developed a variety of approaches for incorporating BEICFs into their management of operational risk (eg risk and control self-assessments, key risk indicators), most consider the application of BEICFs in the risk measurement system as the most challenging of the four required AMA elements. Most banks have developed methodologies to capture key BEICFs, but few are currently able to substantiate how they quantify the impact of those factors on the capital calculation. As a consequence, the practice for many banks is still very much in its formative stages.

One of the current applications of BEICFs is in the development of scorecards, the results of which are used to assess operational risk drivers and controls at a bank's chosen level of granularity and then adjust the measured operational risk capital amount on the basis of these assessments. Another is as part of the risk identification process in the development of operational risk scenarios. A much less common practice is the use of BEICFs as a direct statistical input or adjustment within the AMA model.

V. Data issues

Definition / scope

The nature and quality of operational risk data collected by an AMA bank affect not only the outcome of the bank's quantification process but also its operational risk management decisions. As a result, Basel II prescribes certain standards a bank's operational risk data must satisfy before the bank will qualify for an AMA. These standards relate principally to the characteristics of the data, how it is collected and how it is used. The purpose of the standards is to provide some insight into supervisors' minimum expectations regarding data integrity and comprehensiveness, both of which are critical to the effective implementation of an AMA.

AMA operational risk data can be grouped into the following four categories: internal data, external data, scenario data and data related to a bank's business environment and internal controls. This section of the paper focuses primarily on internal and, to a lesser extent, external data; issues regarding scenarios and business environment and internal controls are addressed principally in the section on modelling/quantitative issues. Much of the discussion that follows relates to paragraph 673 of Basel II regarding the standards applicable to internal loss data. The topics covered include issues regarding:

- the nature of internal loss data that is collected (eg whether near misses and opportunity costs are included, where to draw the line between operational and credit risk losses and how to determine the appropriate gross loss amount for certain types of losses);
- the timing of loss recognition, and;

- the classification of internal losses (eg how losses are allocated over time and across business lines and event types).

AMA operational risk data has multiple applications, including risk quantification, risk management and accounting and other forms of reporting. Some data are suitable for more than one application, whereas other data are single-purpose. Although this paper does not explicitly distinguish among these different applications, it addresses issues that arise in all of them.

Relative to internal governance and modelling, the other subject areas covered in this paper, data issues lend themselves more naturally to surveys. Consequently, internal surveys of AIGOR members provided much of the material for the range of practice outlined in the discussion that follows.

Specific topics and corresponding practices

i. Date of occurrence of internal losses

Frequently, operational risk losses are not identified by the affected bank until months after the date of their occurrence. A question then arises about the date that a bank should assign to such losses within its internal loss database.

Basel text

"[A] bank should collect information about the date of the event …The level of detail of any descriptive information should be commensurate with the size of the gross loss amount." (paragraph 673, third bullet)

Issues/background

While Basel II requires AMA banks to record the date of an event, it does not provide any additional guidance. Choices about the date of occurrence of a large internal loss can have a significant impact on the assessment of a bank's operational risk profile at a given point in time and over time. The most appropriate date is not always self-evident, however, which could lead to differences in practice across banks and corresponding differences in capital calculations, particularly where large losses are involved. Banks' practices in this area tend to be strongly influenced by accounting or provisioning practices, which could generate results that are inconsistent with a bank's true operational risk profile.

Litigation cases provide a good illustration of the issue. Litigation cases often take years to resolve such that the relevant business line often will have introduced appropriate risk mitigation techniques by the time a case is concluded. If a bank uses the accounting date for the loss event for purposes of calculating operational risk capital, the sudden increase in capital allocated to the relevant business line may undermine the internal credibility of the allocation framework. On the other hand, there are concerns that an early public recognition of potential settlements of individual litigation cases could increase the likelihood and size of legal losses.

Range of practice

In practice, banks generally assign one of three dates to an individual operational risk loss: date of occurrence, date of discovery or accounting date. Of the three, banks tend to favour the date of occurrence or date of discovery over the accounting date. Litigation cases are a notable exception for which banks lean towards the accounting date or the date on which the case is settled, if different from the accounting date. This may be related to banks'

preference for the ‘certainty’ criterion in the accounting guidance for recognising such expenses in some jurisdictions and concerns about early public recognition of potential settlements increasing the likelihood and size of legal losses.

ii. Evaluation methods for internal losses

The gross amount of an internal loss can usually be determined readily – but this is not always the case. For example, vastly different amounts can be estimated in respect of damage to physical assets depending on whether book value, market value or replacement cost is used. Whether to include overtime costs incurred to fix system failures is another example of decisions that impact gross loss amounts.

Basel text

”Aside from information on gross loss amounts, a bank should collect …” (paragraph 673, third bullet)

Issues/background

Basel II does not elaborate on the definition of ‘gross loss’. Different practices can result in big differences in gross loss amounts for the same event, particularly in the case of damage to physical assets where the amounts in question can be substantial.

Because damaged physical assets have to be repaired or replaced, it could be argued that the gross loss amount should reflect some measure of the extent to which an asset’s economic value is impaired, in which case replacement cost or market value might be appropriate. Quite often, however, replacement cost and market value are not readily available and cannot be estimated objectively. In contrast, while book value may deviate from an asset’s economic value, it is accessible and leaves less room for widely divergent results as it relies on established accounting guidance. A bank’s choice of practice will influence how it validates the losses and affect the supervisory review process. In that regard, the use of book value for capital calculation purposes makes validation a straightforward matter, while the difference between book and economic value could still be used in a bank’s assessment of its exposure to operational risk. Irrespective of the practice that is followed, the capital treatment of damage to physical assets under an AMA may also be affected by how such assets are treated in the credit risk component of Basel II.

Similar issues arise with respect to decisions about the treatment of overtime costs, although the amounts in question will generally be much smaller than those involving damage to fixed assets.

Range of practice

Banks generally use one of the following three options for evaluating damage to physical assets for operational risk management and measurement purposes: book value, market value or replacement cost. Currently, banks’ practices seem to be evenly divided among the three options.

Many banks validate these losses by reconciling the amounts with their general ledger, although this validation technique may only be relevant where book values are used for the loss amount. Other banks rely on risk control or audit functions to validate these loss amounts.

As for overtime costs for fixing systems failures, many banks do collect this information for operational risk management and measurement purposes.

iii. Internal losses that materialise over time

Some individual operational risk events result in losses that materialise over a period of time and some operational risk events that occur over a period of time may be triggered by the same root cause. This raises questions about how banks should treat such losses for risk measurement purposes and how they should be reflected in banks' internal loss databases.

Basel text

"A bank must develop specific criteria for assigning loss data arising … from related events over time." (paragraph 673, fourth bullet)

Issues/background

The way in which a bank treats losses that are related but which materialise over a period of time can affect its capital calculation. In some cases, the impact can be material. One example is the case where a series of individual losses related to the same operational risk event falls below a bank's collection threshold but surpasses that threshold when the individual losses are taken together. Because the individual losses would not be recorded, the aggregate loss amount would not be factored into the capital calculation. The higher the loss collection threshold, the greater the potential impact would be.

Another example is the case where multiple loss events occurring over a period of time are triggered by the same root cause. If the possibility that the individual loss events may be correlated is not reflected in the internal loss database, the result could be an underestimate of the bank's risk exposure.

Range of practice

Many banks use the date of the original operational risk event when recording all subsequent loss effects in their internal loss databases. Although practices vary considerably across banks, the following are examples of the criteria banks have developed to identify subsequent loss effects: the identity of offenders; similarity of crime categories; the cause of legal penalties, and a defined period of time over which any damage to physical assets occurs. Typically, the criteria are developed by a bank's risk control function. Many banks cluster all related losses identified using these criteria for risk quantification purposes.

iv. Allocation of internal losses across business lines and event types

An individual operational risk event can lead to losses in multiple business lines and losses arising from a single event can sometimes span multiple event types. As in the case of events that trigger losses over a period of time, questions arise regarding how banks should treat these losses for risk measurement purposes and how they should be reflected in banks' internal loss databases.

Basel text

"A bank must develop specific criteria for assigning loss data arising from an event in a centralised function (eg an information technology department) or an activity that spans more than one business line …" (paragraph 673, fourth bullet)

"Any banking or non-banking activity which cannot be readily mapped into the business line framework, but which represents an ancillary function to an activity included in the framework, must be allocated to the business line it supports. If more than one business line is supported through the ancillary activity, an objective mapping criteria must be used." (Annex 8, paragraph (b))

Issues/background

How a bank allocates losses that occur in a centralised business function or losses from a single operational risk event affecting multiple business lines could affect both its measurement and management of operational risk. For example, allocating a loss across multiple business lines and using this 'disaggregated' data for risk measurement would likely underestimate the risk where the losses were all a result of the same event. From a risk management perspective, the failure to allocate such losses or inappropriate allocation could send the wrong signal to business line management and undermine the internal credibility of the capital allocation process.

Range of practice

Generally, banks have adopted one of two practices in this area: (i) allocating the entire loss to the business line for which the impact is greatest, or (ii) allocating the loss on a pro-rata basis across the affected business lines. In the case of losses from a single event, the former practice seems to have been implemented more widely. Practice is more evenly divided with respect to losses occurring in a centralised function.

v. Collection of gross versus net internal loss amounts

A net internal loss amount is the loss incurred by a bank after taking into account recoveries from clients, insurance or other sources.

Basel text

"Aside from information on gross loss amounts, a bank should collect information about … any recoveries of gross loss amounts … The level of detail of any descriptive information should be commensurate with the size of the gross loss amount." (paragraph 673, third bullet)

Issues/background

Basel II does not define 'gross loss', as noted above, or 'recoveries'. Many recoveries occur on the same day as, and sometimes within minutes of, the related loss. However, months or years can pass before some recoveries are realized. Netting may nonetheless be appropriate in such circumstances if there is certainty about the amount that will be recovered. The timing of a recovery is often among the criteria banks use to determine whether the gross loss amount recorded in their internal loss database and/or used for risk measurement purposes should be net of the amount recovered. Where a full recovery occurs within the timeframe allowed by a bank's netting criteria, the bank would not record a loss event. It is also possible in the case of some types of events (eg erroneous money transfers or settlements with counterparties meeting certain criteria) that no loss would be recorded where a full recovery has not yet occurred but is only anticipated. Because the amounts involved can be significant, different practices among banks can result in big differences in the gross loss amount for similar events, and correspondingly big differences in capital calculations.

Range of practice

Banks generally collect information about recoveries as well as gross loss amounts. In the case of many banks, the gross loss amount recorded in the internal loss database is the actual gross loss amount less any recoveries that occur within a specified period of time. Typically, this period of time ranges from the same day to a few days. Some banks, however, believe that much longer periods might be appropriate in the case of certain types of events

in respect of which full recovery is anticipated based on the nature of the underlying transaction and/or counterparty. In these instances and in cases where losses are fully recovered within the period of time allowed for netting, banks typically do not record that an event has occurred but might record a near miss.

vi. Scope of internal data – near misses and opportunity costs

In the course of designing and implementing processes and systems for collecting operational risk data, AMA banks face decisions about how wide a net to cast for purposes of capturing internal loss data. There is some uncertainty about whether certain types of data, such as near misses and opportunity costs, should be captured, particularly where such data may not constitute operational risk 'losses' or 'events', per se, or where they do not clearly fall within the scope of internal loss data as it is described in Basel II.

Basel text

"Operational risk … includes legal risk, but excludes strategic and reputational risk." (paragraph 644)

"Banks must track internal loss data according to the criteria set out in this section. The tracking of internal loss event data is an essential prerequisite to the development and functioning of a credible operational risk management system." (paragraph 670)

"A bank's internal loss data must be comprehensive in that it captures all material activities and exposures from all appropriate sub-systems and geographic locations." (paragraph 673, second bullet)

Issues/background

Basel II does not state explicitly that AMA banks should collect information about near misses or opportunity costs or, consequently, how this information might be used if it is collected. Given the general scarcity of operational risk loss data, however, near miss and opportunity cost data could be useful in both risk management and measurement. For example, by subjecting such information to management discussion, it could contribute to, and perhaps broaden, management's understanding of a bank's exposure to operational risk and its potential impact. It might also provide additional insight into process improvement opportunities and be relevant in discussions with internal audit. In addition, it could be used to inform the development of scenarios. On the other hand, the relevance of near misses and opportunity costs may not be readily apparent as long as their relationship with operational risk events and losses and their definition remain unclear. Moreover, these types of internal data present incremental measurement and validation challenges and could be both costly and technically difficult to collect in a consistent fashion.

Range of practice

The current practice in this area varies. In general, however, near miss data tend to be collected more broadly than opportunity costs. Among those who do collect near miss data, many define near misses as direct or indirect losses that could have been suffered as a result of an operational failure but which were avoided. Some banks that collect near miss data do so only where the potential loss exceeds a prescribed threshold.

The challenges in collecting near miss data include difficulties in precisely defining the nature of events that constitute near misses. In addition, internal data collection processes typically start with the recognition of a loss event before proceeding to identifying the nature of the operational failure – and by definition, there is no loss event in the case of a near miss.

These challenges affect a bank's ability to systematically collect consistent data about near misses.

Banks that do collect near miss data tend not to use it for risk quantification purposes, although some incorporate the data in scenarios. More generally, banks use near miss data to identify operational risk trends and for other risk management purposes.

vii. Boundary – operational versus credit, market and other risks

Some losses are clearly the result of operational risk. For others, it is less clear whether they should be classified as operational risk or credit, market or strategic risk, for example. In still other cases, it may be appropriate to allocate an individual loss partially to operational risk and partially to credit or some other risk category. These classification issues are broadly described as 'boundary' issues.

Basel text

"Operational risk losses that are related to credit risk and have historically been included in banks' credit risk databases (eg collateral management failures) will continue to be treated as credit risk for the purposes of calculating minimum regulatory capital under this Framework. Therefore, such losses will not be subject to the operational risk capital charge …." (paragraph 673, fifth bullet)

"Operational risk losses that are related to market risk are treated as operational risk for the purposes of calculating minimum regulatory capital under this Framework and will therefore be subject to the operational risk capital charge." (paragraph 673, sixth bullet)

"Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk." (paragraph 644)

Issues/background

Basel II is relatively clear regarding the operational risk-market risk boundary but leaves more room for interpretation regarding the operational risk-credit risk boundary. In particular, it is silent regarding the treatment of operational risk losses, that are related to credit risk, but which have not historically been included in banks' credit risk databases. In addition, while operational risk is defined to exclude strategic and reputational risks, neither of the latter two risk types are defined.

Basel II incorporates different approaches for estimating capital requirements for different types of risk. As a result, a given loss event could produce very different capital outcomes depending on its risk classification. This could lead to differences in the treatment of similar losses between banks and inappropriate estimates of a given bank's operational risk exposure.

The absence of clear boundaries between loss types also presents opportunities for regulatory capital arbitrage, inducing banks to game their risk classification of losses. For example, an AMA bank that implements FIRB for credit risk purposes could arbitrage the boundary by shifting large losses from operational risk, where they might otherwise increase the regulatory capital requirement, to credit risk, where they would have no impact on regulatory capital as LGD is fixed for FIRB banks. Conversely, a TSA bank that implements AIRB for credit risk purposes could be motivated to shift large losses from credit to operational risk, where they would have no impact on regulatory capital. Finally, because the boundaries between operational risk and strategic and reputational risks are unclear, an

AMA bank might have room to game the boundaries and simply omit large losses from the regulatory capital calculation.

The industry and supervisors have done a considerable amount of work on these definitional issues. In practice, however, the boundaries between different risk types are often neither clear nor broadly shared within the banking or supervisory communities.

Range of practice

At this juncture, it would seem that banks have a relatively clear concept of the operational risk-market risk and operational risk-credit risk boundaries. For example, banks generally intend to treat market risk losses caused by traders who violate loss or risk limits as operational risk, and not market risk, for capital calculation purposes. In the case of loan-related losses caused by operational events such as inadequate or failed processes, banks generally intend to treat them as credit risk for Basel II capital calculation purposes even though they have not been treated as credit risk losses or included in banks' credit risk databases historically.

Credit card fraud is an interesting case to consider given the large losses many banks experience in this area and, therefore, the potential impact boundary decisions could have on a bank's capital calculation. The practice in this area would appear to be evenly split between banks that treat all types of credit card fraud as operational risk, on the one hand, and those that treat third party-initiated fraud as operational risk and all other types of credit card fraud as credit risk on the other.

Banks employ a variety of practices to distinguish operational risk from credit and market risk. For example, decision trees have been developed by some banks. Some banks use higher loss collection thresholds as a means of narrowing down the number of boundary cases that need to be assessed.

There seems to be less of a consensus developing among banks regarding the distinction between operational and strategic risk. While many banks regard losses arising from inappropriate business decisions by senior management as strategic risk losses, many others treat such losses as operational risk. Some banks have yet to develop a clear definition of strategic risk for internal risk management purposes.

viii. Internal loss collection thresholds

Loss collection thresholds are *de minimis* levels below which loss amounts are not collected or recorded in a bank's internal loss database.

Basel text

"A bank must have an appropriate *de minimis* gross loss threshold for internal loss data collection, for example €10,000. The appropriate threshold may vary somewhat between banks and within a bank across business lines and/or event types. However, particular thresholds should be broadly consistent with those used by peer banks."

Background/issues

The choice of loss collection thresholds can significantly affect the calculation of expected loss and, to some extent, the shape of the estimated loss distribution and estimates of unexpected loss. Where reconciliation with the general ledger may be considered beneficial, higher thresholds can make it more difficult to reconcile expected loss estimates with the general ledger. All else being equal, the more loss data that is collected the greater will be

the opportunity for precision in the estimates. There is a trade-off, however, between the added benefits for risk estimation from collecting smaller losses and the cost of collecting such information. Striking the right balance has proven challenging.

Range of practice

Most banks tend to rely on expert judgement rather than more empirical methods to set loss collection thresholds. In some cases, banks choose certain thresholds because they have been in use for some time. In others, business line managers and risk quantification experts contribute their views based on their understanding of the business and the impact of the threshold on the risk quantification process. Most banks use the same threshold for all business lines, although many have introduced different thresholds for different business lines.

Some banks have set thresholds but have chosen nonetheless to collect data under the threshold. In the case of many of these banks, these data are used to analyse expected loss. Some banks include such losses in their capital calculation but do not collect the same detailed information about these losses as they do for losses above the threshold.

ix. Mapping of internal loss data to 8x7 matrix

Internal operational risk loss data can be broadly categorized along two dimensions, business line and event type. The Basel II business line and event type categories form an 8x7 matrix into which a bank can map its internal losses.

Basel text

"To assist in supervisory validation, a bank must be able to map its historical internal loss data into the relevant level 1 supervisory categories defined in Annexes 8 and 9 and to provide these data to supervisors upon request. It must have documented, objective criteria for allocating losses to the specified business lines and event types. However, it is left to the bank to decide the extent to which it applies these categorizations in its internal operational risk measurement system." (paragraph 673, bullet 1)

Issues/background

There is no requirement for banks to map their internal loss data into the standard 8x7 matrix on an ongoing basis. But while there is little debate regarding the requirement that banks 'be able to' map their internal loss data into the standard 8x7 matrix, there remains some question regarding the degree of standardisation that should be required.

There are advantages and disadvantages to highly standardising the way in which banks classify operational risk losses for the purpose of reporting to supervisors. Standardisation assists supervisors in benchmarking exercises and identifying outlier banks for closer examination. It also enables the pooling and subsequent analysis of data from different banks. On the other hand, standardisation comes at a cost, particularly for banks that use a different business line and/or event type breakdown for internal management purposes. As such, it could deter banks from classifying operational risk loss data in a manner that more accurately reflects the way they manage their business.

Range of practice

Banks' approaches to classifying their internal loss data vary from country to country, in part reflecting differences in view within the supervisory community. Some banks have developed their own matrix for classifying operational risk losses, whereas others use the standard 8x7

matrix from Basel II. The in-house matrix developed by some banks uses a business line breakdown based on a client rather than product dimension. Some banks have developed an in-house matrix based on causes rather than events.

x. Validation of internal loss data

The validation of internal loss data refers to the steps banks take to assess the comprehensiveness and overall integrity of their internal loss data and the integrity of the data collection process.

Basel text

"Internal and/or external auditors must perform regular reviews of the operational risk management processes and measurement systems. This review must include both the activities of the business units and of the independent operational risk management function." (paragraph 666(e))

"Banks must track internal loss data according to the criteria set out in this section. The tracking of internal loss event data is an essential prerequisite to the development and functioning of a credible operational risk management system. Internal loss data is crucial for tying a bank's risk estimates to its actual loss experience …." (paragraph 670)

"Internal loss data is most relevant when it is clearly linked to a bank's current business activities, technological processes and risk management procedures. Therefore, a bank must have documented procedures for assessing the ongoing relevance of historical loss data, including those situations in which judgement overrides, scaling, or other adjustments may be used, to what extent they may be used and who is authorised to make such decisions." (paragraph 671)

"Internally generated operational risk measures used for regulatory capital purposes must be based on a minimum five-year observation period of internal loss data, whether the internal loss data is used directly to build the loss measure or to validate it. When the bank first moves to the AMA, a three-year historical data window is acceptable (this includes the parallel calculations in paragraph 46)." (paragraph 672)

"A bank's internal loss data must be comprehensive in that it captures all material activities and exposures from all appropriate sub-systems and geographic locations. A bank must be able to justify that any excluded activities or exposures, both individually and in combination, would not have a material impact on the overall risk estimates ...."(paragraph 673, second bullet)

Issues/background

Validation entails a review and assessment of both the process for collecting data and the contents of the internal loss database. It encompasses both data integrity and data comprehensiveness and involves issues such as missing or incomplete data and how a bank treats data from abandoned lines of business. The periodic validation of internal loss data is essential to promoting appropriate risk management decisions and ensuring that the results of the quantification process are meaningful and reliable. Given that banks only started to collect internal loss data relatively recently, methodologies for validating internal loss data are still in their infancy and a common industry practice is yet to emerge.

Range of practice

The following practices are among those used by banks as a means of assessing the comprehensiveness and integrity of their internal loss data: (i) reconciliation to the general ledger; (ii) reviews by the risk control function, including consistency checks across various internal reports (eg loss reports, control self-assessments); (iii) reviews by internal and external audit; (iv) examinations of inconsistencies in loss data across entities or business lines within the bank; (v) features embedded in the loss data collection system such as pop-up user guides and decision trees; (vi) use of a centralised function to input internal loss data into the data repository, and; (vii) exception reports that are circulated to the relevant business lines and vetted by the risk control function.

When banks judge their internal data to be insufficient for risk measurement purposes, most supplement it with external data or scenario analysis, although both approaches introduce the need for additional validation work.

Bank practice also varies when it comes to dealing with internal loss data from abandoned lines of business. Some maintain a history of the data from abandoned lines of business in their internal loss databases for future reference, as necessary. Some banks exclude the data when they are able to conclude that there is no possibility of new losses arising from the abandoned line of business.

xi. External loss data – sources and relevance

External loss data comprises operational risk losses experienced by third parties and information about those losses that banks can use to assess the relevance of a particular loss to their circumstances.

Basel text

"A bank's operational risk measurement system must use relevant external data (either public data and/or pooled industry data), especially when there is reason to believe that the banks is exposed to infrequent, yet potentially severe, losses. These external data should include data on actual loss amounts, information on the scale of business operations where the event occurred, information on the causes and circumstances of the loss events, or other information that would help in assessing the relevance of the loss event for other banks. A bank must have a systematic process for determining the situations for which external data must be used and the methodologies used to incorporate the data (eg scaling, qualitative adjustments or informing the development of improved scenario analysis). The conditions and practices for external data use must be regularly reviewed, documented, and subject to periodic independent review."(paragraph 674)

Issues/background

With the paucity of internal loss data relative to what is required to reasonably assess a bank's operational risk profile, banks are exploring the use of external data to supplement their internal loss data. External loss data is available from various sources, but whatever the source it must be assessed for its relevance and may need to be adjusted depending on how it is used in an operational risk measurement system. For example, for some applications of external data adjustments may be required to account for differences in size, business environment and internal controls. Depending on the external data source, there may be gaps in the information needed to make these adjustments, sometimes due to lack of disclosure by a data vendor or consortium. In addition, work remains to be done before some of the technical challenges to scaling and other adjustments are resolved. These issues are not insignificant as a bank's inappropriate use of external data could have a material impact

on the outcome of its capital calculation. Some banks are reluctant to join data consortia due to confidentiality concerns.

Range of practice

Banks gather external loss data by one or more of the following means: (i) building and maintaining an in-house database by gathering relevant information from public sources such as newspapers, magazines and trade journals; (ii) participating in industry data consortia; and, (iii) purchasing external data from vendors. Consortium data appear to cover a wider range of events than vendor data.

While many banks have access to vendor or consortium data that includes data from their respective countries, this is not universally the case. As a result, some banks would have to gather such external data themselves if it is considered of sufficient importance.

Many banks use external data to inform their scenario process and for risk management purposes such as validation. Some banks use external data as a direct input to a risk quantification model.

VI. Modelling / quantification issues

Definition / scope

The flexibility provided in the AMA reflects the comparative stage of development of operational risk modelling, relative to the modelling of other risk types, and hence the need to allow banks to explore how best to obtain risk-sensitive estimates of operational risk exposure. While the industry has made significant progress in modelling operational risk, limited internal data and significant differences in loss experiences across banks, and across business lines, make it difficult to determine preferred models. Allowing flexibility in modelling allows continued evolution and justifies not being prescriptive in respect of modelling approaches and assumptions.

While flexibility helps promote experimentation on how best to model operational risk, however, it also raises the possibility that banks with similar risk profiles could hold different levels of capital under the AMA if they rely on substantially different modelling approaches and assumptions. Clearly, there exists a trade-off between flexibility and consistent treatment. Consistency within and across jurisdictions will depend on how supervisors view and assess particular modelling approaches as well as on how banks implement supervisory requirements.

This section highlights those areas of operational risk modelling where a wide range of industry practice exists. The focus of this section is on those topics that may have a significant impact on banks' modelled operational risk capital estimates. These topics include:

- the granularity of, and correlation/dependence assumptions in, AMA models;
- the distributional assumptions underpinning operational risk severity and frequency estimates;
- issues associated with the use and combination of the required elements of an AMA model;
- the use of insurance as a risk mitigant; and

- the treatment of expected loss.

While these topics are discussed separately, most of them are intertwined. For example, appropriate modelling of correlation within and across operational risk classes, or units of measure, is integrally tied to how internal data is assembled and the level of granularity in estimating a bank's operational risk exposure. Some of these topics are also closely related to topics covered under the other subject areas, data issues and internal governance. Going forward, supervisors will work on providing further clarity around their assessment processes and, where possible, on refining the range of acceptable practice such that more consistency can be achieved.

Specific topics and corresponding practices

i. Granularity

The granularity of an AMA reflects the degree to which the approach separately models individual operational risk exposures.

Basel text

"A bank's risk measurement system must be sufficiently 'granular' to capture the major drivers of operational risk affecting the shape of the tail of the loss estimates." (paragraph 669(c))

Issues/background

There is considerable diversity across banks in the granularity of approaches to measuring bank-wide operational risk exposure. The least granular approaches are those that use a single risk measurement model for all of a bank's operational risk exposures. These approaches tend to rely on the assumption that operational risk losses are identically distributed, or in other words, that potential operational risk losses are generated from the same statistical distribution. Typically, these less granular approaches also assume the operational risk losses are independent. A key advantage of these approaches is that, in estimating only a single distribution of operational risk losses, operational risk loss data can be pooled, thus helping to address issues related to data paucity. A potential drawback is that they may not reflect the true nature of the underlying losses in that the losses often are not independent.

The most granular approaches are those that estimate potential operational risk losses using a set of models that vary by business line and/or operational risk event type (ie by operational risk class, or unit of measure). Granular approaches provide scope to capture differences in operational risk exposures across business lines or event types and allow correlations between, and sometimes within, these units of measure to be taken into account. In doing so, however, these approaches require a much larger pool of observed operational risk loss data points to estimate statistical distributions for the full range of business lines and/or event types on which the modelling approach is based and to support any assumed correlation structure.

Range of practice

At this time, the granularity of operational risk measurement approaches is wide-ranging from bank to bank. At one end of the spectrum are those banks that have developed one model to estimate the operational risk exposure across the entire organisation. At the other end are those that have implemented separate models for each of the business lines and loss event types over which operational risk is being modelled. In between, there are banks that have

adopted separate models for either different business lines or different operational loss event types. Irrespective of whether one model or a set of models is being used to measure operational risk exposure, most banks have not yet undertaken sufficient statistical or other analysis to support their choice of granularity and the assumptions that that choice of granularity implies, tending to justify the choice of approach only on the basis of data availability.

ii. Correlation and dependence

Correlation is one measure of the dependency of potential operational risk losses across or within business lines and/or loss event types. The concept of correlation can be generalised to more complex dependency relationships (eg copulas) that recognise differences in dependencies across low- and high-severity operational risk events. Dependence structures could occur as a result of business cycles (eg economic difficulties that cause an increase in rogue trading and fraud), firm-specific factors (eg a new senior manager changes the control environment across a number of business lines) or cross-dependence of large events (eg flooding results in widespread looting and increases the number of fraudulent transactions).

Basel text

"Risk measures for different operational risk estimates must be added for purposes of calculating the regulatory minimum capital requirement. However, the bank may be permitted to use internally determined correlations in operational risk losses across individual operational risk estimates, provided it can demonstrate to the satisfaction of the national supervisor that its systems for determining correlations are sound, implemented with integrity, and take into account the uncertainty surrounding any such correlation estimates (particularly in periods of stress). The bank must validate its correlation assumptions using appropriate quantitative and qualitative techniques." (paragraph 669(d))

Issues/background

Banks using less granular approaches to operational risk modelling, that is, those that use a single risk measurement model for all the operational exposures of the bank, usually assume that there are no dependencies between operational risk losses (ie they implicitly assume a correlation of zero). By contrast, banks employing more granular approaches must explicitly assume some form of dependence structure for operational risk losses incurred across those business lines and/or loss event types for which separate operational risk models are used.

A simple approach is to express dependence in terms of a measure of correlation that can range from 0 per cent, which suggests no linear relationship between tail events (ie independence, at least in the case of a joint normal distribution), and 100 per cent, which implies simultaneous occurrence. In general, the higher the correlation that is assumed, the larger will be the operational risk capital outcome.[7] It is also possible to consider more general dependence structures, for which correlation is different between tail and non-tail events and varies within the tail. Complex dependence structures that assume high dependencies between operational risk tail events are particularly important and may lead to

[7] This may not be true for extremely heavy-tailed distributions, such as those with infinite means.

operational risk capital outcomes that are larger than when a 100 per cent correlation assumption is made, although this outcome is unlikely for regulatory capital purposes.[8]

Because much of a bank's estimated operational risk capital is generated through the tail of the distribution, the issue of dependency between large loss events is particularly relevant.

Range of practice

As is the case for granularity, the range of practice for incorporating dependence into operational risk modelling is broad. Generally, banks tend to be clustered in two groups: those that assume that operational risk loss events are independent, in terms of their frequency, severity or both, and those that assume a moderate degree of dependence. It is likely that the clustering in the first group is a consequence of the 'whole-of-bank' approach that many banks have adopted. This is not always the case, however, with some banks using a more granular modelling approach also making an assumption of independence between operational risk loss events. In many cases, the correlation measure is between business lines and/or loss event types rather than within these units of measure. A very small number of banks are considering incorporation of more complex dependence structures; however, in general, this work is still very much in its infancy. To date, most banks have not stress tested their correlation assumptions and have yet to develop a defensible methodology to support the correlation assumptions that have been made.

iii. Modelling technique – distributional assumptions and estimation

Distributional assumptions underpin most, if not all, operational risk modelling approaches and will generally be made in respect of both operational risk loss severity and the frequency of occurrence of operational risk loss events. Important considerations in a bank's choice of modelling technique are the existence and size of the threshold above which data are captured and modelled.

Basel text

"Given the continuing evolution of analytical approaches for operational risk, the Committee is not specifying the approach or distributional assumptions used to generate the operational risk measure for regulatory capital purposes. However, a bank must be able to demonstrate that its approach captures potentially severe 'tail' loss events. Whatever approach is used, a bank must demonstrate that its operational risk measure meets a soundness standard comparable to that of the internal ratings-based approach for credit risk (ie comparable to a one year holding period and a 99.9th percentile confidence interval)." (paragraph 667)

"… A bank must have an appropriate *de minimis* gross loss threshold for internal loss data collection, for example €10,000. The appropriate threshold may vary somewhat between banks and within a bank across business lines and/or event types …." (paragraph 673, second bullet)

[8] Where the loss distribution functions by business lines and/or loss event types are heavy-tailed, it is possible to consider dependence structures for which the operational risk capital outcome exceeds the sum of capital measures calculated separately for each business line and/or loss event. For extremely heavy-tailed distributions, however, such as those with infinite means, superadditivity can occur even in the presence of independence of data.

Issues/background

Modelling of operational risk exposures is still relatively new and a common view of appropriate distributional assumptions for the frequency and severity of operational risk losses is yet to emerge. It is generally accepted that the severity of operational risk loss data tends to be heavy-tailed and methodologies for modelling operational risk must be able to capture this attribute. This is particularly challenging for many banks, as most have relatively scant datasets and few, if any, tail events. With limited data, it is difficult to distinguish between alternative distributional assumptions. It is clear, however, that a bank's choice of assumption will have a significant impact on operational risk capital, as will the statistical method used for fitting that distribution. Similarly, banks' choice of data threshold may impact the amount of the expected loss (EL) offset available to a bank and affect the appropriateness of distributional assumptions or estimation method (in that the operational risk losses being modelled constitute a 'truncated data set').

Range of practice

The basis of all banks' operational risk models is a distribution of operational risk losses. However, there exists significant divergence in the processes for generating that distribution. The distributional assumptions made, the modelling techniques used and the data elements on which the distribution is based are all key sources of variation in approach. The range of distributions assumed for modelling the severity of operational risk losses is diverse, with some of the more granular modelling approaches assuming more than one distributional form aligned to the characteristics of a particular business line or loss type. Distributions used include the generalised Pareto distributions of extreme value theory, empirical distributions, lognormal distributions, heavy-tailed distributions and light-tailed distributions.

There is much less diversity across banks in the range of distributions assumed in estimating the frequency of operational risk losses. The most commonly used distribution for frequency is the Poisson distribution. A much smaller number of banks assume a negative binomial distribution.

With respect to thresholds for loss data collection, some banks decide not to establish a collection threshold and instead aim to collect the full range of operational risk losses for modelling purposes. Other banks define a threshold above which they aim to collect all losses, along with information about those losses (eg business line and causal type), but below which they collect limited or no data (limited data could mean, for example, that loss amounts are collected without any descriptive information about individual losses). Of those banks that collect limited or no data below a threshold, some use statistical techniques designed for situations involving truncated data to estimate their model despite the limited availability or absence of data below the threshold.

iv. Use of scenario analysis

Scenario analysis is a process by which banks consider the impact of extreme but nonetheless plausible events on their operations. As such, it can provide a method for capturing potential tail events that may not have occurred at the bank. Different scenarios can provide a means of stress testing the model. Scenarios can be tailored to the business environment of the bank and capture changes in a banks internal or external situation.

Basel text

"A bank must use scenario analysis of expert opinion in conjunction with external data to evaluate its exposure to high-severity events. This approach draws on the knowledge of experienced business managers and risk management experts to derive reasoned

assessments of plausible severe losses. For instance, these expert assessments could be expressed as parameters of an assumed statistical loss distribution. In addition, scenario analysis should be used to assess the impact of deviations from the correlation assumptions embedded in the bank's operational risk measurement framework, in particular, to evaluate potential losses arising from multiple simultaneous operational risk loss events. Over time, such assessments need to be validated and re-assessed through comparison to actual loss experience to ensure their reasonableness." (paragraph 675)

Issues/background

Scenario analysis is an important component in the estimation of a bank's operational risk exposure. Scenario analysis can be helpful in modelling high-severity events, particularly in instances where internal loss event data is limited and external loss data is used but not as a direct input into the AMA model. It also allows a bank to tailor possible tail events to specific risk exposures that may be specific to its circumstances. Scenario analysis is also helpful because it potentially offers a forward-looking perspective not available when using internal loss event data alone.

The incorporation of scenario analysis in a bank's operational risk modelling framework can vary in many respects, including the rigour with which scenarios are developed, the comprehensiveness and number of scenarios used, the severity of losses reflected in the scenarios, the choice of distribution used to fit the scenarios, the application of maximum loss caps to the fitted distributions and the way scenarios are combined with other data elements. Each of these factors can have a significant impact on a bank's operational risk exposure estimate.

Range of practice

Banks' use of scenario analysis in calculating operational risk exposure varies widely. Some banks do not currently use scenario analysis to generate direct inputs to their operational risk capital calculation, while others base their operational risk capital calculation primarily on scenario analysis. Among the banks that do use scenarios, the following common features can be observed in the range of practice:

- the documentation provided for the scenario analysis process is often less comprehensive than for other aspects of the AMA framework. Currently, there is little guidance available to benchmark scenarios or promote consistency of scenarios across banks.
- the rigour applied to scenario development varies greatly. This can be seen in several areas, including the quantity of scenarios per bank, the level at which the scenarios are devised (eg business line, event type), the number and quality of inputs and data sources that are considered in formulating the scenarios (eg internal data, external data, pending litigation losses, risk scoring schemes) and how scenarios are incorporated into the model.
- certain banks incorporate loss caps into their scenario analysis to limit the size of operational risk losses in their models, which can have a significant effect on capital estimation results.

v. Use of external data

External loss data comprises operational risk losses experienced by third parties and information about those losses that banks can use to assess the relevance of a particular loss to their circumstances. External data can offset the paucity of internal operational risk

loss data in areas where a bank has a potential risk but has not experienced significant losses.

Basel text

"A bank's operational risk measurement system must use relevant external data (either public data and/or pooled industry data); especially when there is reason to believe that the bank is exposed to infrequent, yet potentially severe, losses. These external data should include data on actual loss amounts, information on the scale of business operations where the event occurred, information on the causes and circumstances of the loss events, or other information that would help in assessing the relevance of the loss event for other banks. A bank must have a systematic process for determining the situations for which external data must be used and the methodologies used to incorporate the data (eg scaling, qualitative adjustments or informing the development of improved scenario analysis). The conditions and practices for external data use must be regularly reviewed, documented, and subject to periodic independent review." (paragraph 674)

Issues/background

External data is another important component in the estimation of a bank's operational risk exposure. Similar to scenario analysis, it can be helpful in modelling high-severity events particularly in instances where internal loss event data is limited. It also offers a forward-looking perspective.

The way in which external data is incorporated into the operational risk exposure estimate can vary depending upon the qualitative assumptions the bank makes regarding which external loss events are considered relevant and the degree to which the data are scaled or otherwise adjusted (eg through the use of loss caps) to account for differences in a bank's size or other bank-specific factors. The availability of good external data and its comparability to a bank's own loss experience can result in external data being utilised differently across banks and jurisdictions.

Range of practice

Most banks factor external loss data into their operational risk capital estimates, but the method in which the data are incorporated varies. For example, some banks use the information as a direct statistical input to their models, while others use it as an indirect input (eg using the data as a basis for constructing scenarios). Most banks 'filter' external data to select only those observations that are deemed relevant, and have developed specific criteria for determining the relevance of individual events. While many banks recognise the potential importance of scaling external data to account for firm size and other relevant factors, none have derived a workable scaling methodology. Most banks have invested in a database of external operational risk loss information rather than collating their own external data.

vi. Combination of elements

One of the major distinguishing features of operational risk models is how the models combine internal data, external data, scenario analysis and business environment and internal control factors (BEICFs).

Basel text

"Any operational risk measurement system must have certain key features to meet the supervisory soundness standard set out in this section. These elements must include the use

of internal data, relevant external data, scenario analysis and factors reflecting the business environment and internal control systems." (paragraph 669(e))

"A bank needs to have a credible, transparent, well-documented and verifiable approach for weighting these fundamental elements in its overall operational risk measurement system. For example, there may be cases where estimates of the 99.9th percentile confidence interval based primarily on internal and external loss event data would be unreliable for business lines with a heavy-tailed loss distribution and a small number of observed losses. In such cases, scenario analysis, and business environment and control factors, may play a more dominant role in the risk measurement system. Conversely, operational risk loss event data may play a more dominant role in the risk measurement system for business lines where estimates of the 99.9th percentile confidence interval based primarily on such data are deemed reliable. In all cases, the bank's approach for weighting the four fundamental elements should be internally consistent and avoid the double counting of qualitative assessments or risk mitigants already recognised in other elements of the framework." (paragraph 669(f))

Issues/background

While internal loss event data, relevant external loss data, scenario analysis and factors reflecting the business environment and internal controls must be incorporated into a bank's operational risk measurement system, the Basel II Framework does not require that all four elements be incorporated as direct inputs into an operational risk model. Banks have flexibility in the specific methods used for incorporating the elements. Consistent with the flexibility of the AMA, a bank may place different emphasis on each AMA element in order to more closely reflect its specific loss history and risk profile. However, the elements must be combined in a way that allows the institution to meet the supervisory soundness standard. Banks will also need to consider whether the combination of elements can lead to potential double counting. The different emphasis on individual elements can complicate comparisons across banks.

Range of practice

The combination and weighting of individual elements varies widely across banks. Some banks base their operational risk capital estimate largely – or even solely – on scenario analysis, and incorporate internal and external data only indirectly as inputs to the scenario generation process. Other banks rely heavily on internal data, using external data and scenario analysis only where there are gaps in their own loss experience. Others use internal data to model the frequency of operational risk losses and external data to model loss severity, especially in the tail. Most banks, however, incorporate more than one element directly in their AMA model and some incorporate all four, albeit with varying weights. Interestingly, no bank uses BEICFs as the primary determinant of its operational risk calculation. As indicated above, banks have tended to focus much less on this data element than on the collection of historical data or development of scenarios. As a consequence, practice for many banks is still very much in its formative stages. Where BEICFs are in use, this tends to be in the area of capital allocation rather than as a direct statistical input or adjustment within the operational risk modelling approach. Many banks have not established how to avoid double counting through the combination of elements.

vii. Insurance as a risk mitigant

Insurance is a possible alternative to capital for addressing operational risk, provided banks are able to meet the conditions outlined in Basel II.

Basel text

"Under the AMA, a bank will be allowed to recognise the risk mitigating impact of insurance in the measures of operational risk used for regulatory minimum capital requirements. The recognition of insurance mitigation will be limited to 20% of the total operational risk capital charge calculated under the AMA." (paragraph 677)

Issues/background

Banks may be able to incorporate an adjustment to their operational risk capital estimate to recognise insurance as a risk mitigant. It is important for banks to account for factors such as the probability of coverage, the probability of timely payout, deductibles, insurer default, policy limits for certain events, and the remaining term on the policy. An important issue is the rigour with which banks will be expected to calculate the insurance offset. For example, a bank's insurance offset for a given aggregate exposure estimate may vary depending upon the interplay between individual operational risk losses and the insurance policies that are in place. In such a situation, the offset will depend on whether the aggregate exposure is driven by many small losses that fall below deductibles (in which case the offset would be small), by a few large losses that far exceed the policy limits (in which case the offset will also be limited), or by medium-sized losses (in which the offset may be significant). Thus, it can be argued that calculation of the offset should be embedded within the model at the event level rather than being applied as an *ex post* adjustment.

Range of practice

Banks are at various stages of incorporating insurance as a risk mitigant into their operational risk capital models. Many do not take an insurance offset within their current operational risk framework; of the banks that do, many calculate the offset in a very rough manner. For example, some base the calculated offset on a small number of large losses for which insurance recoveries have been significant, while others seem to have interpreted the regulatory language as indicating that a 20% offset can be taken without much justification. A few banks have embedded the calculation of the insurance offset within the model.

viii. Treatment of expected loss (EL)

In November 2005, the AIGOR released guidance[9] on the treatment of EL clarifying the conditions under which banks could be permitted to calculate operational risk capital in respect of unexpected loss, only.

Basel text

"Supervisors will require the bank to calculate its regulatory capital requirement as the sum of expected loss (EL) and unexpected loss (UL); unless the bank can demonstrate that it is adequately capturing EL in its internal business practices. That is, to base the minimum regulatory capital requirement on UL alone, the bank must be able to demonstrate to the satisfaction of its national supervisor that it has measured and accounted for its EL exposure." (paragraph 669(b))

[9] *The treatment of expected losses by banks using the AMA under the Basel II Framework*, Basel Committee Newsletter No.7 (November 2005).

Range of practice

Since banks have not had much time to react to the November guidance, the range of practice is likely to change over time. Most banks using a loss distribution approach are able to calculate EL from their statistical model. In addition, two areas where banks have argued that losses are predictable and are likely to meet the criteria included in the guidance have been in credit card fraud and securities processing. In both instances, some banks have been able to show with historical data that operational risk losses are quite predictable and can provide an estimation process that would be consistent over time. Reserves for these two loss areas are not permitted in some jurisdictions, while in others banks can either reserve for them currently or are expected to be able to do so in the future.

Annex

Members of the AIG Operational Risk Subgroup

Chairman: Kevin Bailey, Office of the Comptroller of the Currency, United States

Australian Prudential Regulation Authority	Colleen Cassidy Harvey Crapp
Banking, Finance and Insurance Commission, Belgium	Jos Meuleman
Banco Central do Brasil, Brazil	Kathleen Krause Wagner Almeida
Office of the Superintendent of Financial Institutions, Canada	Abhilash Bhachech Catherine Pearce
French Banking Commission	Duc Pham-Hi
Deutsche Bundesbank, Germany	Karsten Stickelmann
Federal Financial Supervisory Authority (BaFin), Germany	Jochen Kayser
Reserve Bank of India	Krishnamurti Damodaran
Bank of Italy	Marco Moscadelli
Bank of Japan	Tsuyoshi Nagafuji Tsuyoshi Oyama
Financial Services Agency, Japan	Shinichiro Shimizu
Surveillance Commission for the Financial Sector, Luxembourg	Didier Bergamo
Netherlands Bank	Claudia Weigand
Bank of Spain	María Ángeles Nieto
South African Reserve Bank	Jan van Zyl
Finansinspektionen, Sweden	Anders Broman
Swiss Federal Banking Commission	Martin Sprenger
Financial Services Authority, United Kingdom	Vincent Baritsch Andrew Sheen
Board of Governors of the Federal Reserve System, United States	Stacy Coleman
Federal Deposit Insurance Corporation, United States	Mark Schmidt
Federal Reserve Bank of Boston, United States	Eric Rosengren
Federal Reserve Bank of New York, United States	Ronald Stroz
Office of the Comptroller of the Currency, United States	Mark O'Dell
Office of Thrift Supervision, United States	Eric Hirschhorn
Financial Stability Institute	Juan Carlos Crisanto
Secretariat of the Basel Committee on Banking Supervision, Bank for International Settlements	Jeff Miller