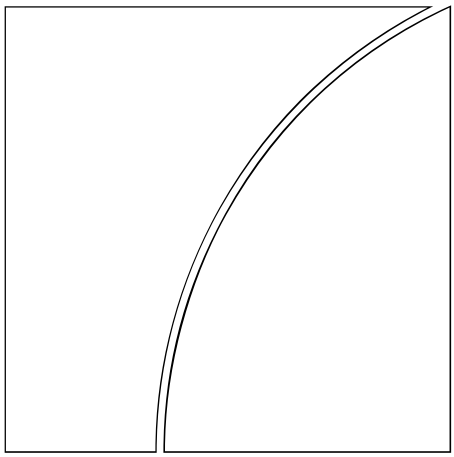
Basel Committee
on Banking Supervision



Sound Practices for the Management and Supervision of Operational Risk

December 2001

BANK FOR INTERNATIONAL SETTLEMENTS

Risk Management Group
of the Basel Committee on Banking Supervision

Chairman:
Mr Roger Cole – Federal Reserve Board, Washington, D.C.

Banque Nationale de Belgique, Brussels	Ms Dominique Gressens
Commission Bancaire et Financière, Brussels	Mr Jos Meuleman
Office of the Superintendent of Financial Institutions, Ottawa	Mr Jeff Miller
Commission Bancaire, Paris	Mr Laurent Le Mouël
Deutsche Bundesbank, Frankfurt am Main	Ms Magdalene Heid Ms Karin Sagner
Bundesaufsichtsamt für das Kreditwesen, Bonn	Mr Jürgen Dreymann
Banca d'Italia, Rome	Mr Claudio Dauria Mr Sergio Sorrentino
Bank of Japan, Tokyo	Mr Eiji Harada
Financial Services Agency, Tokyo	Mr Hirokazu Matsushima
Commission de Surveillance du Secteur Financier, Luxembourg	Mr Davy Reinard
De Nederlandsche Bank, Amsterdam	Mr Klaas Knot
Banco de España, Madrid	Mr Guillermo Rodriguez-Garcia Mr Juan Serrano
Finansinspektionen, Stockholm	Mr Jan Hedquist
Sveriges Riksbank, Stockholm	Ms Camilla Ferenius
Eidgenössiche Bankenkommission, Bern	Mr Daniel Sigrist
Financial Services Authority, London	Mr Helmut Bauer Mr Victor Dowd
Bank of England, London	Ms Alison Emblow
Federal Deposit Insurance Corporation, Washington, D.C.	Mr Mark Schmidt
Federal Reserve Bank of New York	Ms Beverly Hirtle Mr Stefan Walter
Federal Reserve Board, Washington, D.C.	Mr Kirk Odegard
Office of the Comptroller of the Currency, Washington, D.C.	Mr Kevin Bailey Ms Tanya Smith
European Central Bank, Frankfurt am Main	Mr Panagiotis Strouzas
European Commission, Brussels	Mr Michel Martino Ms Melania Savino
Secretariat of the Basel Committee on Banking Supervision, Bank for International Settlements	Mr Ralph Nash

Table of Contents

Sound Practices for the Management and Supervision of Operational Risk

The purpose of this paper, prepared by the Risk Management Group of the Basel Committee on Banking Supervision (the Committee), is to further the Committee's dialogue with the industry on the development of Sound Practices for the Management and Supervision of Operational Risk. Comments on the issues outlined in this paper would be welcome, and should be submitted to relevant national supervisory authorities and central banks and may also be sent to the Secretariat of the Basel Committee on Banking Supervision at the Bank for International Settlements, CH-4002 Basel, Switzerland by 31 March 2002. Comments may be submitted via e-mail: BCBS.capital@bis.org[1] or by fax: + 41 61 280 9100. Comments on this paper will not be posted on the BIS website.

Introduction

1. Deregulation and globalisation of financial services, together with the growing sophistication of financial technology, are making the activities of banks (and thus their risk profiles) more diverse and complex. Developing banking practices at internationally active banks suggest that risks other than credit and market risk can be substantial:

- If it is not properly controlled, the use of more highly automated technology has the potential to transform risks from manual processing errors to system failure risks, as greater reliance is placed on globally integrated systems;

- Growth of e-commerce brings with it potential risks (e.g., external fraud and system security issues) that are not yet fully understood;

- Large-scale mergers, de-mergers and consolidations test the viability of new or newly integrated systems and have resulted in some noteworthy problems;

- The emergence of banks acting as very large-volume service providers creates the need for continual maintenance of high-grade internal controls and back-up systems;

- Banks may engage in risk mitigation techniques (e.g., collateral, credit derivatives, and asset securitisations) to optimise their exposure to market risk and credit risk, but which in turn may produce other forms of risk; and

- The growing use of outsourcing arrangements and the participation in third-party run clearing systems can mitigate some risk but can also present significant other risks to banks.

---

[1] Please use this e-mail address only for submitting comments and not for correspondence.

2. Under the present Accord, these other risks are covered implicitly in the capital buffer related to credit risk. Banks themselves typically hold capital in excess of the current regulatory minimum and some are already allocating economic capital for operational and other risks. However, while many banks have a framework for identifying, monitoring and controlling operational risk, operational risk measurement frameworks remain in a developmental stage.

3. The Committee is proposing to encompass explicitly risks other than credit and market risk in the revised Accord. This will achieve a more comprehensive and sensitive approach to addressing risk at individual institutions, while ensuring that the overall level of capital in the banking sector is maintained at an appropriate level. The Risk Management Group of the Committee set out its current thinking on the framework for an operational risk charge in its *Working Paper on the Regulatory Treatment of Operational Risk*, published in September 2001. In framing the current proposals for a minimum regulatory capital charge for operational risk, the Committee has adopted a common industry definition, namely: 'the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events'. The definition includes legal risk but it excludes strategic, reputational and systemic risks.

4. This definition focuses on the causes of operational risk and the Committee believes that this is appropriate for risk management including, ultimately, measurement. The Committee recognises that for internal purposes banks may choose to adopt their own definitions. It is important that, whatever definition is used, the full range of operational risks facing the bank are considered. Annex 2 of the September Working Paper contains a detailed breakdown of operational risk into a number of event types. This framework has formed the basis of the Committee's data collection exercise (the Quantitative Impact Study) on operational risk and was developed following close consultation with a large number of industry participants.

5. This paper focuses on operational risk, a subset of 'other risks'. Other risks were defined by the Committee on an exclusionary basis, as all risks other than credit, market and interest rate risks. The Committee recognises that operational risk is a substantial element of 'other risks', and is an area where banks themselves are devoting considerable attention and resource. Operational risk lends itself more easily to quantification, and hence effective management, than some other elements of other risk. Nevertheless, banks should seek to manage all significant banking risks, and supervisors will review them as part of the Supervisory Review Process (Pillar 2) of the New Basel Capital Accord.

6. This paper outlines a set of principles, which provide a framework for the effective management and supervision of operational risk, for use by internationally active banks and supervisory authorities when evaluating operational risk management policies, procedures and practices. Whilst the guidance in this paper is intended to apply to internationally active banks, some supervisors may choose to also apply the guidance to those banks deemed significant (e.g., on the basis of size, complexity, or systemic importance) or to smaller, less complex banks.

7. Part 2 of the paper discusses the key elements of a comprehensive operational risk program, which is appropriate for the largest, most sophisticated institutions and which is consistent with emerging industry practice.

8. The Committee recognises that the exact approach chosen by an individual bank will depend on a range of factors, including its size and sophistication and the nature and complexity of its activities. Despite these differences, however, good management information systems, a strong internal control culture and contingency planning are all crucial elements of effective operational risk management for banks of any size and scope. The

Committee's previous paper *A Framework for Internal Control Systems in Banking Organisations* (September 1998) underpins its current work in the field of operational risk.

Industry Trends and Practices

9. In its work on the supervision of operational risks, the Committee has aimed to develop a greater understanding of current industry trends and practices for managing operational risk. These efforts involved numerous meetings with banking organisations, surveys of industry practice, and analyses of the results. Based upon these sources of information, the Committee believes that it has a good understanding of both the banking industry's current range of practices as well as the industry's efforts to develop methods for managing operational risks.

10. In the past, banks relied almost exclusively upon internal control mechanisms within business lines and by the audit function to manage operational risk. While these remain important, recently there has been an emergence of specific structures, tools and processes aimed at managing operational risk. In this regard, an increasing number of organisations have concluded that a risk-sensitive operational risk management programme provides for bank safety and soundness and protects and enhances stockholder value, and are therefore making progress in addressing operational risk as a distinct risk exposure similar to their treatment of credit and market risk.

11. While the approaches for managing operational risk are evolving rapidly, the Committee recognises that there is still much work to be done. For example, the progress towards a standard operational risk definition is somewhat hampered by differences in interpretations across banks. Further, the ability of banks to quantify operational risk varies greatly. Therefore, the Committee believes an active exchange of ideas between the supervisors and industry is key to ongoing development of appropriate guidance for managing exposures related to operational risk.

12. The first part of this paper is organised around the following key areas: (a) developing an appropriate risk management environment; (b) risk management: identification, measurement, monitoring and control; (c) the role of supervisors and (d) the role of disclosure.

Part 1: Sound Practices for the Management and Supervision of Operational Risk

13. In developing these sound practices, the Committee has drawn upon its existing work on the management of other significant banking risks, such as credit and liquidity risk, and the Committee believes that similar rigour should be applied to the identification, measurement, monitoring and control of operational risk. Nevertheless, it is clear that operational risk differs from other banking risks in that it is typically not directly taken in return for an expected reward, but exists in the natural course of corporate activity, and that this impacts the risk management process. In common with its work on other banking risks, the Committee has structured this sound practice paper around a number of principles. These are as follows:

Developing an Appropriate Risk Management Environment

Principle 1: The board of directors[2] should be aware of the major aspects of the bank's operational risks as a distinct and controllable risk category and should approve and periodically review the bank's operational risk strategy. The strategy should reflect the bank's tolerance for risk and its understanding of the specific characteristics of this risk category. The board should also be responsible for approving the basic structure of the framework for managing operational risk and ensuring that senior management is carrying out its risk management responsibilities.

Principle 2: Senior management should have responsibility for implementing the operational risk strategy approved by the board of directors. The strategy should be implemented consistently throughout the whole banking organisation, and all levels of staff should understand their responsibilities with respect to operational risk management. Senior management should also have responsibility for developing policies, processes and procedures for managing operational risk in all of the bank's products, activities, processes and systems.

Principle 3: Information flows within the banking organisation play a key role in establishing and maintaining an effective operational risk management framework. Communication flows within the bank should establish a consistent operational risk management culture across the bank. Reporting flows should enable senior management to monitor the effectiveness of the risk management system for operational risk, and also enable the board of directors to oversee senior management performance.

Risk Management: Identification, Measurement, Monitoring, and Control

Principle 4: Banks should identify the operational risk inherent in all types of products, activities, processes and systems. Banks should also ensure that before new products, activities, processes and systems are introduced or undertaken the operational risk inherent in them is subject to adequate assessment procedures.

Principle 5: Banks should establish the processes necessary for measuring operational risk.

Principle 6: Banks should implement a system to monitor, on an on-going basis, operational risk exposures and loss events by major business lines.

Principle 7: Banks should have policies, processes and procedures to control or mitigate operational risk. Banks should assess the costs and benefits of alternative risk limitation and control strategies and should adjust their operational risk exposure using appropriate strategies, in light of their overall risk profile.

---

[2] This paper refers to a management structure composed of a board of directors and senior management. The Committee is aware that there are significant differences in legislative and regulatory frameworks across countries as regards the functions of the board of directors and senior management. In some countries, the board has the main, if not exclusive, function of supervising the executive body (senior management, general management) so as to ensure that the latter fulfils its tasks. For this reason, in some cases, it is known as a supervisory board. This means that the board has no executive functions. In other countries, by contrast, the board has a broader competence in that it lays down the general framework for the management of the bank. Owing to these differences, the notions of the board of directors and senior management are used in this paper not to identify legal constructs but rather to label two decision-making functions within a bank.

Role of Supervisors

Principle 8: Banking supervisors should require banks to have an effective system in place to identify, measure, monitor and control operational risks as part of an overall approach to risk management.

Principle 9: Supervisors should conduct, directly or indirectly, regular independent evaluation of a bank's strategies, policies, procedures and practices related to operational risks. Supervisors should ensure that there are effective reporting mechanisms in place which allow them to remain apprised of developments at banks.

Role of Disclosure

Principle 10: Banks should make sufficient public disclosure to allow market participants to assess their operational risk exposure and the quality of their operational risk management.

I. Developing an Appropriate Risk Management Environment

14. An effective operational risk strategy should implement an operational risk management process and ensure effective board and senior management oversight. The formality and sophistication of the operational risk management process should be commensurate with the risk incurred by the bank.

Principle 1: The board of directors[2] should be aware of the major aspects of the bank's operational risks as a distinct and controllable risk category and should approve and periodically review the bank's operational risk strategy. The strategy should reflect the bank's tolerance for risk and its understanding of the specific characteristics of this risk category. The board should also be responsible for approving the basic structure of the framework for managing operational risk and ensuring that senior management is carrying out its risk management responsibilities.

15. The board of directors should address explicitly operational risk as a distinct and controllable risk to the bank's safety and soundness. Failure to address operational risk, which is present in virtually all bank transactions and activities, may greatly increase the likelihood that some risks will go unrecognised and uncontrolled. The board may address operational risk in part by approving a definition of operational risk that clarifies those risks that the bank has decided it can manage internally and those that it may wish to be transferred.

16. The board should approve a bank-wide operational risk strategy and establish a management structure capable of implementing that strategy. The strategy should define explicitly the bank's level of risk tolerance and how the bank will keep risks within that level, including specific lines of responsibility. The board should review the strategy regularly to ensure that the bank is managing the operational risks arising from external market changes and other environmental factors, as well as those operational risks associated with new products, activities or systems. This review process should also aim to incorporate industry innovations in operational risk management into the bank's systems and processes. If necessary, the board should revise the operational risk management framework in light of this analysis to ensure that material operational risks are captured within the framework.

17. Banks should have in place adequate internal audit coverage to verify that operating policies and procedures are effectively implemented.[3] The board - either directly, or indirectly through its audit committee - should ensure that the scope and frequency of the audit programme is appropriate to the risks involved. To the extent that the audit function is involved in this process, the board should ensure that the independence of the audit function is maintained. This independence may be compromised if the audit function is directly involved in the operational risk management process.

Principle 2: Senior management should have responsibility for implementing the operational risk strategy approved by the board of directors. The strategy should be implemented consistently throughout the whole banking organisation, and all levels of staff should understand their responsibilities with respect to operational risk management. Senior management should also have responsibility for developing policies, processes and procedures for managing operational risk in all of the bank's products, activities, processes and systems.

18. Management must translate the operational risk management strategy established by the board of directors into policies, processes and procedures that can be implemented and verified. While each level of management is responsible for the appropriateness and effectiveness of policies, processes, procedures and controls within its purview, senior management must clearly assign authority, responsibility and reporting relationships to encourage this accountability. This responsibility includes ensuring that the necessary resources are available to manage operational risk effectively. Moreover, senior management should assess the appropriateness of the management oversight process in light of the risks inherent in a business line's strategy and ensure that staff are apprised of their responsibilities.

19. Senior management should ensure that bank activities are conducted by qualified staff with the necessary experience and technical capabilities and that staff responsible for monitoring and enforcing the institution's risk strategy have authority independent from the business units they oversee.

20. Senior management should also ensure that the bank's remuneration policies reflect its risk strategy. Remuneration policies that reward staff that deviate from policies (e.g. by exceeding established limits) weaken the bank's risk management processes.

21. Integrated objectives among managerial levels are particularly crucial for banks using, or in the process of implementing, advanced technologies to support high transaction volumes. Particular attention should be given to the quality of documentation controls and to transaction-handling practices. Policies, processes and procedures related to such technologies should be well-documented and disseminated to all relevant personnel.

Principle 3: Information flows within the banking organisation play a key role in establishing and maintaining an effective operational risk management framework. Communication flows within the bank should establish a consistent operational risk management culture across the bank. Reporting flows should enable senior management to monitor the effectiveness of the risk management system for operational risk, and also enable the board of directors to oversee senior management performance.

---

[3] The Committee's paper, *Internal Audit in Banks and the Supervisor's Relationship with Auditors* (August 2001) describes the role of internal and external audit.

22. The board of directors and senior management, at their respective responsibility levels, must communicate that the management of operational risk is an institutional priority. Senior management should communicate to all staff its risk management expectations, and maintain effective channels of communication to ensure that staff understand fully and adhere to the policies, processes and procedures affecting their duties and responsibilities. An explicit operational risk management strategy helps the board to communicate clearly its expectations to senior and other management and to hold management accountable for meeting those expectations.

23. Specific consideration should be given to co-ordinating internal communications. It is vital that operational risk managers communicate effectively with their counterparts in other areas, such as those dealing with credit or market risk, as well as with the department(s) responsible for the procurement of external services, such as insurance purchasing and outsourcing agreements.

24. In order to assess accurately risk exposures against risk tolerances stated in the board's strategy and adherence to internal policies, processes and procedures, senior management should receive regular reports from both business units and the internal audit function. The reports should contain internal financial, operational and compliance data, as well as external market information about events and conditions that are relevant to decision making. Reports should be distributed to appropriate levels of management and areas of the bank where topics of concern may have an impact. Reports should reflect fully any identified problem areas and should motivate timely corrective action on outstanding issues. To ensure the usefulness and reliability of these risk and audit reports, management should regularly verify the timeliness, accuracy and relevance of reporting systems and internal controls in general. Management may also use reports prepared by external sources (auditors, supervisors) to assess the usefulness and reliability of internal reports. Reports should be analysed with a view to improving existing risk management performance as well as developing new risk management policies, procedures and practices.

II. Risk Management: Identification, Measurement, Monitoring and Control

Principle 4: Banks should identify the operational risk inherent in all types of products, activities, processes and systems. Banks should also ensure that before new products, activities, processes and systems are introduced or undertaken the operational risk inherent in them is subject to adequate assessment procedures.

25. Risk identification is critical for the subsequent development of viable operational risk measurement, monitoring and control. Effective risk identification considers both internal factors (such as the complexity of the bank's structure, the nature of the bank's activities, the quality of personnel, organisational changes and employee turnover) and external factors (such as fluctuating economic conditions, changes in the industry and technological advances) that could adversely affect the achievement of the bank's objectives.

26. The risk identification process should also include a determination of which risks are controllable by the bank and which are not. There are several processes commonly used by banks to help them identify operational risk:

- Self- or Risk-Assessment: a bank assesses its operations and activities against a menu of operational risk events. This process is internally driven and often incorporates checklists and/or workshops to identify the strengths and weaknesses of the operational risk environment.

- Risk Mapping: in this process, various business units, organisational functions or process flows are mapped by risk type. This exercise can reveal areas of weakness and help prioritise subsequent management action.

- Key Risk Indicators: risk indicators are statistics and/or metrics, often financial, which can provide insight into a bank's risk position. These indicators should be reviewed on a periodic basis (often monthly or quarterly) to alert banks to changes that may be indicative of risk concerns. Such indicators may include for example the number of failed trades, staff turnover rates and the frequency and/or severity of errors and omissions.

- Threshold/limits: typically tied to risk indicators, threshold levels (or changes) in key risk indicators, when exceeded, alert management to areas of potential problems.

- Scorecards: these provide a means of translating qualitative assessments into quantitative metrics that can be used to allocate economic capital to business lines in relation to performance in managing and controlling various aspects of operational risk.

Principle 5: Banks should establish the processes necessary for measuring operational risk.

27. Measuring operational risk requires both estimating the probability of an operational loss event and the potential size of the loss. All banks should engage in tracking group wide operational risk data. Such information is fundamental to measuring, monitoring and controlling operational risk exposure. For any reliable measurement system, data would need to be collected in order to develop general measures of operational risk. While the nature of the data collected may vary across banks, to be useful, the breadth, history and integrity of the data collected must be commensurate with the bank's operational risk profile and approach to managing risk.

28. Under this principle, banks should develop sound internal reporting practices and systems that are consistent with the scope of operational risk defined by supervisors and the banking industry. In addition, banks should have an operational risk measurement methodology, knowledgeable staff and an appropriate systems infrastructure capable of identifying and gathering operational risk data.

Principle 6: Banks should implement a system to monitor, on an on-going basis, operational risk exposures and loss events by major business lines.

29. An effective monitoring process is essential for adequately managing operational risk. Ongoing monitoring activities can offer the advantage of quickly detecting and correcting deficiencies in the policies, processes and procedures for managing operational risk. Promptly detecting and addressing these deficiencies can substantially reduce the potential severity of a loss event.

30. The frequency of monitoring should reflect the risks involved and the frequency and nature of changes in the operating environment. Monitoring is most effective when the system of internal control is integrated into the bank's operations and produces regular reports. The results of these monitoring activities should be included in management and board reports, as should compliance reviews performed by the internal audit and/or risk management functions. Supervisory reports may also inform this monitoring and should likewise be reported internally.

Principle 7: Banks should have policies, processes and procedures to control or mitigate operational risk. Banks should assess the costs and benefits of alternative risk limitation and control strategies and should adjust their operational risk exposure using appropriate strategies, in light of their overall risk profile.

31. Control activities are designed and implemented to address the risks that the bank has identified. For those risks that are controllable, the bank must decide the extent to which it wishes to use control procedures and other appropriate techniques or bear the risk. For those risks that cannot be controlled, the bank must decide whether to accept these risks or to withdraw from or reduce the level of business activity involved. Control processes and procedures should be established and banks should have a system in place for ensuring compliance with a documented set of internal policies concerning the risk management system. Principal elements of this could include:

- top-level reviews of the bank's progress towards the stated objectives;
- checking for compliance with management controls;
- policies, processes and procedures concerning the review, treatment and resolution of non-compliance issues; and
- a system of documented approvals and authorisations to ensure accountability to an appropriate level of management.

32. To be effective, control activities should be an integral part of the regular activities of a bank, and should involve all levels of personnel in the bank, including both senior management and business unit personnel. Controls that are an integral part of the regular activities enable quick responses to changing conditions and avoid unnecessary costs.

33. An effective internal control system also requires that there be appropriate segregation of duties and that personnel are not assigned responsibilities which may create a conflict of interest. Assigning such conflicting duties to individuals, or a team, may enable them to conceal losses, errors or inappropriate actions. Therefore, areas of potential conflicts of interest should be identified, minimised and subject to careful independent monitoring and review.

34. Some significant operational risks have low probabilities but potentially very large financial impact. Risk mitigation tools or programs can be used to reduce the exposure to such events. However, banks should view these as complementary to, rather than a replacement for, thorough internal operational risk control, as an important mitigation technique is the timely internal resolution of errors. Having mechanisms in place to quickly recognise and rectify legitimate operational risk errors can greatly reduce exposures. Careful consideration also needs to be given to whether a risk mitigation strategy is truly reducing risk, or merely transferring the risk to another business sector or area. One growing risk mitigation technique is the use of insurance to help mitigate operational risk. Innovative insurance policies with prompt and certain pay-out features could be used to externalise the risk of “low frequency, high severity” losses which may occur as a result of events such as errors and omissions, physical loss of securities, employee or third-party fraud, and natural disasters.

35. Investments in appropriate processing technology and information technology security are also important for risk mitigation. However, banks should be aware that increased automation can transform high-frequency, low-severity losses into low-frequency, high-severity losses. The latter may be associated with loss or extended disruption of services caused by internal factors or by factors beyond the bank’s immediate control (e.g.,

external events). Such problems may cause serious difficulties for banks and could jeopardise an institution's ability to conduct key business activities. This potential requires that banks establish business resumption and contingency plans that take into account different types of plausible scenarios, including disruption to communication technology, to which the bank may be vulnerable.

36. Banks should also establish sound policies for managing the risks associated with outsourcing activities. Clearly, the outsourcing of activities has the potential to enhance the bank's performance and can reduce the institution's risk profile by transferring activities to others with greater expertise and scale to manage the risks associated with specialised business activities. Outsourcing activities should be based on rigorous legal agreements ensuring a clear allocation of costs between external service providers and the outsourcing bank. Furthermore, banks need to manage and control any residual risks associated with outsourcing arrangements, including disruption of services or reputational risks.

37. Depending on the importance and criticality of the activity, banks should understand the potential impact on their operations and on their customers of any potential deficiencies in services provided by vendors and other third-party service providers, including both operational breakdowns and the potential business failure or default of the external parties. The extent of the external party's liability and financial ability to compensate the bank for errors, negligence and other operational failures should be explicitly considered as part of the risk assessment. Banks should carry out due diligence tests and monitor the activities of third party providers, especially those lacking experience of the banking industry's regulated environment. For critical activities, the bank may need to consider contingency plans, including the availability of alternative external parties and the costs and resources required to switch external parties, potentially on very short notice.

III. Role of Supervisors

Principle 8: Banking supervisors should require banks to have an effective system in place to identify, measure, monitor and control operational risks as part of an overall approach to risk management.

38. The New Basel Capital Accord has sought to encourage better risk management by establishing operational risk as a distinct risk category, subject to a minimum capital requirement in Pillar 1, and as a focus for the supervisory review process under Pillar 2. To the extent that banks can demonstrate to supervisors increased sophistication and precision in their management of operational risk, banks are expected to move into more advanced approaches, which will generally result in a reduction of the operational risk capital requirement. By setting appropriate criteria for the more advanced approaches to operational risk the Committee believes it can create an incentive for increasingly effective risk management. Furthermore, these criteria give supervisors a sound basis for assessing the adequacy of operational risk management.

39. Pillar 2 is an integral and critical component of the New Basel Capital Accord and directly complements the Pillar 1 operational risk capital charge. Pillar 2 is intended not only to ensure that banks have adequate capital to support all risks in their business, but also to encourage banks to develop and use better techniques in managing those risks. Pillar 2 strongly emphasises the importance of bank management developing an internal capital assessment process and setting targets for capital that are commensurate with the bank's particular risk profile and control environment. This internal process will be subject to supervisory review and, where appropriate, intervention. Supervisors should consult with the internal and external auditors, as appropriate, to determine the adequacy of the risk assessment methodology used by the bank. In cases where supervisors determine that a

bank's operational risk management is either inadequate or ineffective for that bank's specific risk profile, supervisors should require improvements along with the possibility of an interim additional capital buffer for operational risk, consistent with Pillar 2 of the New Basel Capital Accord.

Principle 9: Supervisors should conduct, directly or indirectly, regular independent evaluation of a bank's strategies, policies, procedures and practices related to operational risks. Supervisors should ensure that there are effective reporting mechanisms in place which allow them to remain apprised of developments at banks.

40. The independent evaluation of operational risk by supervisors under Pillar 2 should incorporate a review of the following:

- The bank's process for assessing overall capital adequacy for operational risk in relation to its risk profile and its internal capital targets;
- The effectiveness of the bank's risk management process and overall control environment with respect to operational risk exposures;
- The bank's systems for monitoring and reporting operational risk exposures and other data quality considerations;
- The bank's procedures for the timely and effective resolution of operational risk exposures and events;
- The bank's process of internal controls, reviews and audit to ensure the integrity of the overall operational risk management process; and
- The effectiveness of the bank's operational risk mitigation efforts.

41. Supervisors should also seek to ensure that, where banks are part of a financial group, there are procedures in place to ensure that operational risk is managed in a consistent and proportionate way across the group. In performing this assessment, co-operation and exchange of information with other supervisors may be necessary. Some supervisors may choose to use external auditors in these assessment processes.

42. Deficiencies identified during the supervisory review may be addressed through a range of actions. Supervisors should use the tools most suited to the particular circumstances of the bank and its operating environment. In order that supervisors receive current information on operational risk, they may wish to establish reporting mechanisms, directly with banks and external auditors.

43. Given the general recognition that operational risk management processes are still in development at most banks, supervisors should take an active role in encouraging ongoing internal development efforts by inquiring about and evaluating a bank's recent improvements and plans for prospective developments. These efforts can then be compared with those of other banks to provide the bank with useful feedback on the status of its own work. Further, to the extent that there are identified reasons why certain development efforts have proven ineffective, such information could be provided in general terms to assist in the planning process. In addition, supervisors should focus on the extent to which a bank has integrated the operational risk management process throughout its organisation to provide clear lines of communication and responsibility and encourage active self assessment of existing practices and cost-benefit analysis of possible risk mitigation enhancements.

IV. Role of Disclosure

Principle 10: Banks should make sufficient public disclosure to allow market participants to assess their operational risk exposure and the quality of their operational risk management.

44. Pillar 3 of the New Basel Capital Accord emphasises the importance of market discipline in supporting minimum capital requirements and the supervisory review process. The Committee believes that timely and frequent public disclosure of information by banks can lead to enhanced market discipline.

45. The area of operational risk disclosure is not yet well established, primarily because banks are still in the process of developing operational risk management techniques. The Committee believes that where a bank has a sound operational risk management framework that identifies, measures, monitors and controls operational risk in an effective manner, then disclosure of such a framework will prove beneficial to the bank in accessing the markets and will improve the effective allocation and pricing of capital. In September, the Transparency Group of the Basel Committee published a working paper on Pillar 3, which set out disclosure requirements for operational risk. The Committee will be consulting further on Pillar 3 in future.

Part 2: Supervisory Guidance for a Comprehensive Operational Risk Management Programme

I. Introduction

46. The additional guidance in this Part is a supplement to Part 1 and is intended to apply to the largest, most complex banks with significant operational risk exposures, or to those designated by national supervisors. It reviews banks' efforts to develop a comprehensive, risk-sensitive operational risk management infrastructure to assure that operational risks are properly identified, measured, monitored and controlled. The purpose of this Part is to provide banking supervisors and banks with additional information about operational risk that they should take into account when assessing risk management practices, particularly when applying the Advanced Measurement Approaches (AMA) for regulatory capital assessment or when developing techniques for internal economic capital assessment.

47. Supervisors recognise that processes for managing operational risk are evolving and want to encourage continued innovation. However, it is also clear that a comprehensive, bank-wide operational risk programme should comprise certain fundamental quantitative and qualitative elements that complement each other. It therefore is appropriate to present the essential elements of a sound advanced operational risk management programme at this time, along with the recent gains in understanding that have emerged in the industry. The Committee recognises that few banks have in place all of the elements of an operational risk programme and that this paper presents emerging sound practices gleaned from a number of leading banks that are devoting significant resources to the development of bank-wide operational risk management and capital assessment frameworks. The Committee may elect to issue more detailed guidance in the future in response to the ongoing development of more sophisticated tools for managing operational risk by industry participants.

II. Management Structure and Responsibilities

48. Discussions with many banks with diversified business activities indicate that operational risk is a very important component of their overall risk profiles. At a number of banks, operational risk is considered to rank second only to credit risk in terms of risk exposure and may be greater than market risk (for example, when measured in terms of economic capital allocations). In some banks that focus on asset management or payments and processing activities, however, operational risk may present the largest potential loss exposure to the bank.

49. Against this background, leading banks have, or are in the process of putting in place, clearly defined organisational structures for managing operational risk that are comparable with existing structures for market and credit risk and which, in principle, reflect a decision-making process that sets policy on a centralised basis (generally working closely with affected business lines) and executes it on a decentralised basis. Given the often blurred distinctions between operational, credit, and market risk it is an emerging sound practice for banks to enhance coordination across the market, credit and operational risk management areas.

50. Banks' management structures and responsibilities for operational risk vary, but a number of themes are emerging at the leading banks. Many banks have established an independent operational risk management function at the corporate level that has a direct reporting line to senior management (e.g., the Chief Risk Officer). An emerging practice at leading banks is to rationalise the potentially overlapping responsibilities of various operational risk management committees and activities by forming a bank-wide operational risk committee or unit with a designated head of operational risk. The head of operational risk may, in turn, participate in a bank-wide risk committee that includes credit and market risk and can provide an effective forum to coordinate risk management activities and address potential gaps or overlaps.

51. As there are a variety of staff functions that play important roles in operational risk management, the head office operational risk committee or unit generally establishes a working protocol with, for example, the units responsible for information technology, human resources, legal and insurance purchasing (as an operational risk mitigant). Institution-specific factors will play an important role in establishing an appropriate protocol. The motivation for establishing such a function is to obtain a clear picture of bank-wide operational risk exposure and implement ways to manage this risk. Typical responsibilities for the corporate operational risk function include:

- Establishing consistent definitions for operational risk across the bank's business units;
- Developing bank-level policies, procedures and practices to ensure that operational risk is appropriately identified, measured, monitored and controlled;
- Producing bank-level operational risk exposure reports and forward-looking key risk and performance indicators or scorecards for senior management;
- Overseeing and ensuring the integrity of the operational risk assessment process within the business lines;
- Implementing and maintaining the bank's economic capital assessment and allocation methodologies for operational risk; and

- Developing strategies for mitigating operational risk, possibly in conjunction with risk-mitigating products such as operational risk insurance, outsourcing, operational risk derivatives and pooling arrangements.

52. In addition to establishing a bank-wide perspective on operational risk, an effective operational risk management structure is grounded in the insights and expertise of the business line managers. The operational risk management functions typically work closely with the business lines to implement bank-level policies. In many cases, the operational risk management function has independent operational risk managers within each of the major business lines whose responsibility is to assess risks at the ground level and ensure that corporate risk management policies are put in practice.

53. As is the case for market risk and credit risk, management in each of the business lines will have a much more detailed understanding of business processes and the primary points of vulnerability that may result in significant operational risk exposures. In many banks, business line managers are responsible for developing tracking measures for the major sources of operational risk, reporting any issues or findings to the independent operational risk management functions and putting in place appropriate controls.

54. Finally, as discussed in Part 1, internal and external audit play an important role in a comprehensive operational risk management programme. It is an emerging sound practice for the operational risk management function to oversee the bank-wide operational risk management programme and for the audit function to assess whether this function is truly independent and whether it is effectively implementing the policies and procedures specified by the board of directors and senior management.

III. Defining Operational Risk

55. As discussed in Part 1 of this paper, the foundation of an effective operational risk management programme is a clear understanding throughout the bank of what constitutes operational risk. Clear definitions of the elements of operational risk promote communication among risk management units by providing a means to distinguish operational risk types from market and credit risk, thereby clarifying accountability. Operational risk definitions and classifications provide a foundation for comprehensive, bank-wide management of operational risk.

56. In recent years, the banking industry has expended considerable effort deliberating ways in which operational risk can usefully be identified and categorised. Although there is no formal industry consensus on a single approach, there is considerable agreement among a number of banks on a framework, including supporting definitions. Without mandating a single approach, there is growing consensus that a common framework that could serve as the basis for the creation of pooled reference databases would be extremely useful to individual banks and to the industry as a whole.

57. The causal definition of operational risk discussed in the introduction to this paper is particularly useful for the discipline of managing operational risk within the business lines as it seeks to identify why losses happen and breaks the source of losses down by people, processes, systems, and external factors. For the purpose of bank-wide quantification of operational risk, however, as well as for the pooling of data across banks, it is necessary to rely on definitions that are readily measurable and comparable. Given the current state of industry practice, this has led banks and supervisors to distinguish between operational risk causes, operational risk loss events (measurable losses which may be due to a number of causes, many of which may not be fully understood), and the operational risk loss effects that are reflected in a bank's profit-and-loss (P&L).

58. It is an emerging sound practice among leading banks to use a loss classification approach for managing operational risk. While classification systems vary across banks, they generally encompass loss event types such as internal and external fraud; employment practices and workplace safety; clients, products, and business practices; damage to physical assets; business disruptions; system failures; and execution, delivery, and process management. Many banks further sub-divide these categories to more clearly identify the types of events giving rise to operational risk losses.

59. Focusing on operational risk events enables banks to categorise their actual loss experience in a comprehensive framework and distinguish more clearly operational risk from market and credit risk. This approach also provides a framework that corresponds to the way that many banks structure their risk management activities. By assigning losses into distinct categories according to the general nature of the operational risk event, banks are able to assess the impact of risk mitigating activities – such as enhanced internal controls and processes – intended to reduce the likelihood and severity of such events. In that way, a loss classification system both highlights the type of events that can lead to significant losses and provides direct and meaningful information about the need for and effectiveness of various risk management measures.

60. Aside from categorising operational risk losses by event or risk type, it is also a common practice to classify losses across a bank's major business lines. This process creates a two-way "matrix" classification system that assigns losses to various business line/event type cells. The specific business lines utilized may vary from bank to bank. As a point of reference, the Committee, working with the industry, has developed the following broad categories that can be utilized by a fairly wide range of banks: corporate finance; trading and sales; retail banking; commercial banking; payment and settlement; agency services and custody; asset management; and retail brokerage. As with the event type classification systems, many banks further sub-divide these categories into business lines that reflect their particular structure and mix of business activities. Some banks also find it useful to categorise losses according to their effects, which allows banks to track and categorise these losses in terms that are consistent with a bank's general ledger accounting system, thereby linking the loss categorisation to the bank's P&L attribution process. Loss effect categories typically include elements such as legal liability, regulatory action, loss or damage to physical assets, restitution, loss of recourse, and write-downs. For any given loss event, this classification system allows a bank to track the P&L impact of the event in a way that maps directly into its overall P&L accounts.

IV. Operational Risk Data Collection

61. An essential foundation for any rigorous operational risk management process is comprehensive, reasonable, verifiable and validated data covering the historical operational risk loss experience of the bank. The discipline of collecting loss data is not only needed to understand the dimensions of risk the bank faces but can also be used to motivate staff to consider and more actively control key elements of risk. The discipline of bank-wide data collection promotes a dialogue within the bank about determining the major operational risk exposures and drivers and reinforces more qualitative efforts to manage operational risk within each of the business lines. Thus, it is a sound practice for banks to have a framework for collecting data on their actual operational risk loss experience within material business lines; indeed, it is a qualifying criterion for the use of the AMA approaches under Pillar 1.

62. Operational risk loss data consists primarily of routine, generally high-frequency, low-impact events, as well as low-frequency, high-impact events. Leading banks have implemented reporting systems to track both types of loss events, including reference to external data on large loss events. Average, or expected, losses at a bank are generally

driven by the high-frequency, low-impact events. These expected losses generally should be budgeted with a high degree of confidence and routinely flow through the income statement, although this may not be the case in all business lines (e.g., e-commerce). In contrast, unexpected losses – which tend to reflect the impact of low-frequency, high impact events – occur infrequently and are sometimes sufficiently large as to result in a periodic loss and reduction in tier one capital. Statistically, the expected losses can be thought of as the mean of a loss distribution and the unexpected losses as "tail" events. The latter, unexpected losses are the primary focus of the supervisory and capital allocation processes for operational risk.

63. As discussed in detail in the AMA qualifying criteria, banks should have clear policies and procedures that establish standards for data integrity and comprehensiveness, specify how data is to be collected, and provide the authority (and under what circumstances) to make changes to internal and external data sets that are used in the bank-wide economic capital methodology.

64. In the case of low-frequency, high-severity losses, banks may need to supplement their internal data with industry loss data. Banks should have policies in place describing the circumstances in which such external data are to be collected, their relevance to the bank and how they are to be used within the bank. The standards should address circumstances when a bank's internal loss experience is not sufficiently robust to arrive at a meaningful estimate of the tail of the loss distribution, along with reasonable approaches for scaling external data to the bank's own activities. External loss data can usefully include not only information on actual loss amounts, but also information on the causes and circumstances of the event itself.

65. Industry efforts to begin pooling loss data based on more robust and granular definitions by business lines and event types should enable banks to arrive at better measures of their potential exposure to lower-frequency, higher-severity operational risk events. The Committee recognises that the use of external data for operational risk management purposes is a relatively new area and encourages continuing rapid development of methodologies for incorporating external data into banks' measurement of operational risk.

V. Operational Risk Measurement: Internal Capital Assessment and Allocation

66. The consultative document on "Pillar 2 (Supervisory Review Process)" issued in January 2001 as part of the second consultative package on the New Basel Capital Accord specified supervisory expectations for banks' internal capital assessments. Specifically, banks are expected to have a process for assessing *overall* capital adequacy in relation to their risk profiles—taking into account all material risks—and a strategy for maintaining their capital levels.

67. A key element in developing a credible estimate of overall economic capital needs is an assessment of the potential operational risk losses that the bank could face at a reasonable soundness standard. Meaningful economic capital assessments and allocations across business lines can help identify which businesses are truly profitable and therefore increase shareholder value. Failure to assess capital for operational risk, on the other hand, may result in a distorted picture of the bank's overall risk profile, its capital needs and its return on economic capital at the bank and business line levels. Moreover, if operational risk is not being measured adequately within the bank, this can create incentives to engage in risk mitigation activities that reduce market and credit risk but increase operational risk. Finally, the absence of a clear framework for assessing capital for operational risk results in reduced transparency about the total economic capital a bank holds and makes it difficult for

supervisors, bank managers, investors and counterparties to understand the bank's internal capital adequacy assessment.

68. Against this background, the process for arriving at the total economic capital number for operational risk at the bank-wide and business line levels should be based on reasonable and transparent assumptions that lend themselves to validation, both internally and by supervisors. A critical starting point for any such process, as discussed in the previous section, is a clear definition of risk events that are considered within the operational risk framework. At the broad level, a bank should communicate its economic capital assessment for operational risk throughout the organisation. It is also important that banks make clear which elements are measured and which are determined in a more subjective fashion (e.g., a cushion for strategic risk and/or reputational risk).

69. In recent years, there has been rapid innovation in banks' operational risk measurement methodologies and economic capital assessment techniques. Annex 4 of the September 2001 working paper discussed a number of techniques that currently are in use, and others are likely to evolve in the future. Against a background of rapid innovation, this section discusses the major conceptual elements of a comprehensive operational risk economic capital assessment framework that are being developed at leading banks, as well as some of the key issues that banks and supervisors will need to address going forward. The elements discussed here are:

- Quantitative approaches to assessing bank-wide operational risk capital;
- Qualitative assessments; and
- Validation techniques.

70. It should be noted that this represents a stylised discussion, with a certain degree of overlap across the three above elements. It also should be noted that banks vary in terms of their emphasis across these three broad elements, reflecting differing conceptual views about the appropriate way to manage operational risk.

Quantitative approaches to assessing bank-wide operational risk capital

71. In recent years, many banks have developed or are in the process of developing more quantitative, in many cases statistical/probabilistic, methodologies to help them assess the amount of economic capital that should be attributed to operational risks at the bank and business line levels. While somewhat of a generalisation, the industry appears to be moving from top-down methodologies to more granular, bottom-up approaches that are built up from the business line and/or risk factor levels. Some banks are combining top-down and bottom-up approaches to assess bank-wide economic capital needs.

Top down approaches

72. Top-down methodologies have tended to focus on broader measures of operational risk at the bank level. In this regard, banks have experimented with a variety of types of methodologies. Some have simply focused on the total amount of capital needed to attain a target credit rating. In addition, these banks may have developed techniques for assessing explicitly credit and market risk capital, attributing the residual to operational risk. Others have applied broad measures such as fixed expenses or gross revenues as a proxy for operational risk, in some cases benchmarking off peer institutions when calibrating their internal capital charge. Others have relied on publicly available external loss data, scaling relevant external losses to the size of their bank, as a means to obtain a rough estimate of potential tail event losses.

73. Banks that have applied such top-down methodologies have noted a number of difficulties associated with this approach, including the lack of risk sensitivity of the broad measures and the difficulty of making the link between broad bank and industry measures and the actual risk exposure within the business lines. In the case of approaches relying on public loss data, banks have had difficulties scaling the data to their particular contexts (i.e., it is generally only possible to scale by total assets). In addition, banks have struggled to make these measures relevant to the risk management and decision making processes of business line managers.

Bottom up approaches

74. Recent industry efforts have focused on developing more granular operational risk quantification techniques, beginning at the level of the business lines and building up to a bank-wide measure of risk and the associated necessary capital. There is a significant degree of innovation and development currently underway in this area of operational risk measurement and various bottom-up methods are currently being developed and implemented.

75. Banks using a bottom-up methodology frequently rely on estimates of risk exposures at the business line level. These estimates are generally derived from models that attempt to capture the probability distribution of operational risk losses over some future time horizon (for instance, one year). The models used vary in the complexity and nature of their underlying assumptions, from fairly simple approaches based on the probability and average severity of operational risk events to more sophisticated methodologies that attempt to estimate the shape of the "tail" of the loss distribution. As was discussed in more detail in Annex 4 of the September *Working Paper on the Regulatory Treatment of Operational Risk*, banks may use a variety of approaches to estimate the tail of the loss distribution, including loss distribution and scorecard approaches or combinations of the two. Likewise, some banks have used scenario analysis (subject to certain assumptions about the shape of the probability distributions) to estimate exposure to low frequency events.

76. A common theme across many of these measurement methodologies is the desire to adequately capture the rare, but potentially quite severe, operational risk events that can drive operational risk capital assessments using some kind of statistical analysis. These methodologies can be used to assess capital within business lines or risk types. In addition, banks are working to aggregate business line or risk type loss estimates to arrive at a bank-wide assessment of the operational risk loss exposure at some assumed confidence level and risk horizon.

77. Banks that are developing these techniques should consider a range of issues. These include, but are not limited to:

Data

- As discussed in the previous section, banks may not have much internal data for certain low frequency operational risk loss types. In these situations, what criteria are appropriate for determining when it is necessary to supplement internal loss data with additional (external) data? What data is relevant and what methodology should be used to scale external data to the internal context? How much weight should be given to external versus internal data?

- In those cases where internal data are available, how does historical data relate to the likely future loss experience of the bank? How do changes in the scale of operations, business mix, and/or internal controls affect this relationship?

- If the bank uses scenario analysis as a means to address data insufficiency, how does one develop reasonable assumptions for the scenario generating process? How might one use external data to validate the reasonableness of judgements used to generate scenarios?

Statistical methodology

78. There are many possible methodologies that banks could use to estimate the tail of the distribution, including empirical techniques, various types of assumed loss distributions, extreme value theory, and scenario analysis (based on certain distributional assumptions). Different approaches may result in very different results. More work is needed to assess the assumptions underlying different measurement approaches and how they impact resulting capital estimates. More work is also needed to determine criteria for choosing among different estimation techniques (parametric, Monte Carlo, etc.) for a given sample of loss data. In addition, critical assumptions such as whether operational risk losses are non-linear with respect to size, frequency, and/or severity require more study, as they have a major impact on the estimate of the tail of the loss distribution.

Portfolio effects

79. When aggregating the bottom-up operational risk loss estimates to arrive at a bank-wide capital measure, a number of banks have made assumptions about the correlations among different dimensions of operational risk. More work is needed to understand the relationships among operational risk losses across business lines and event types, both across banks and over time. More thought also needs to be given to the underlying process that generates operational risk losses, for example, whether there are certain systematic factors that cause certain losses to be correlated or whether one can assume that operational risk losses generally are idiosyncratic.

Qualitative Assessments

80. Many leading financial institutions have attempted to supplement *statistical* estimates of operational risk capital with *qualitative* assessments of a bank's operational risk exposure, including in particular an evaluation of the risk management and control environment. While largely based on judgement (versus statistical analysis of actual or assumed loss distributions) such qualitative assessments typically are translated into a quantitative metric that can be incorporated into the bank's risk management process. Over time, the link between statistically based measures and qualitative factors is likely to become tighter as banks study the relationships among actual historical loss experience and judgement-based risk indicators.

81. There are two broad considerations that have motivated banks to embed qualitative factors in their economic capital assessment methodologies. First, banks and supervisors recognise that there are limitations to the backward-looking perspective of an approach that relies exclusively on historical internal loss experience. Improvements in quality control, technology and risk management processes can produce significant differentiation among banks and within a bank over time in terms of loss experience rates for specific business line activities and loss event types. Perfunctory reliance on internal and external data sources can be misleading in such cases. To the extent that the industry loss experience is broadly reflective of a bank's internal risk profile, incorporating such external data into a bank's measurement framework may introduce some degree of forward-looking emphasis (e.g. in the case of new business lines). Nevertheless, these approaches can only gradually reflect in the economic capital charge possible changes in a bank's risk profile due to factors such as new business activities, greater business volume or improvement (deterioration) in the control environment. The shortcoming of a purely data-based approach is particularly acute

for low frequency, high severity operational risk types, where many years of data would be required to detect actual changes in a bank's risk profile. Indeed, it can be argued that the likelihood of a certain type of "tail event" recurring may be lower because a bank would take immediate steps to improve its operational controls and risk mitigation strategies in response to any high-severity operational risk loss event. Thus, reflecting in a qualitative manner ongoing improvements (or deterioration) in a bank's risk management and business environment can provide a forward-looking perspective on likely deviations from the historical loss experience.

82. The second motivation for supplementing historical loss data with qualitative assessments of operational risks is to create additional positive incentives, rewards and penalties for risk and business managers to engage in desirable behaviours that contribute to the reduction of bank-wide operational risk exposures. In recent years, many banks have made significant investments to develop qualitative frameworks to manage operational risk at the business line level. Many banks use such qualitative assessment techniques as a major factor in allocating capital across business lines, thus creating a closer link between the bank-wide capital planning objectives and the risk management and control efforts within the business lines.

83. Against this background, a number of banks are developing transparent metrics to adjust capital amounts over time in relation to the risk-taking and risk-mitigating actions taken within individual business lines. Transparency can be achieved by enabling business lines to understand *ex ante* how certain actions would translate into allocated capital for a given area. This can help business managers balance the costs associated with new investments in risk management against potential capital savings related to a reduction in the operational risk exposure.

84. Banks have developed a range of approaches to making these qualitative assessments, typically based on some combination of self assessments, key risk indicators and scorecards. In some cases, banks attempt to isolate indicators that serve as proxies for how well the bank is managing the frequency and severity of losses. Other indicators are intended to measure the inherent riskiness of a given business line for a given level of controls. Yet other indicators may be intended to capture changes in the overall control environment, both within and across business lines.

85. Many banks are considering how best to relate statistical assessments of economic capital (based on internal, external, and/or simulated loss experience) with qualitative operational risk assessment techniques such as self assessments, key risk indicators, and scorecards, which have been used for monitoring risks and controls at the business line level for a number of years. There is significant diversity across the industry as to how the statistical measures and the qualitative assessments are being integrated. Some banks continue to have concerns about the robustness of qualitative, judgement-based factors and have limited the scope for such adjustments within their statistical measurement methodologies. On the other end of the spectrum, some banks have placed less emphasis on statistical, loss data-based methods when assessing an overall capital number for the bank, focusing more on changes in a given capital number and allocations across business lines using qualitative measures. A plurality of banks appear to fall in the middle of these two ends of the spectrum, working on bottom-up quantification measures that incorporate historical loss data (internal and external) and scenario analysis, as well as qualitative factors to allocate capital to business lines and address changes in the bank's risk profile over time.

86. Banks implementing qualitative assessment approaches should consider a number of issues, including, among others:

- Identifying a meaningful set of operational risk indicators. In the absence of causal analysis that shows the relationship between actual loss experience and movements in risk indicators, this will be largely a judgmental exercise, drawing on the experience of business line managers.

- Determining the appropriate relationship among indicators. For example, should certain indicators be given more weight than others? Should the weighting for a given set of indicators differ among business lines? Are certain indicators correlated (within and across business lines and risk types)?

- Assessing whether the size and direction of quantitative adjustments based on qualitative factors are correct and reasonable. For example, do these adjustments, individually and in combination, continue to produce risk estimates with the desired soundness standard? Are the relationships between qualitative assessments and risk estimates stable over time?

- Determining the appropriate balance between historical, statistical-based approaches and qualitative assessment approaches. For example, some banks have considered placing upper and lower bounds on the degree to which statistical loss measures could be adjusted based on qualitative factors. Other banks are using the statistical measures to determine an initial bank-wide capital number and are using measures such as scorecards to measure changes in this initial capital number over time. In the latter case, how frequently should the initial bank-wide capital assessments be recalibrated?

Validation

87. Whichever broad approach or combination of approaches a bank uses to assess and allocate economic capital for operational risk, it is important that there be a critical review of the assumptions driving the key parameters of these operational risk measurement methodologies. In order to validate the reasonableness of the methodologies, a bank should demonstrate that its risk measurement processes are properly structured and that the resulting risk estimates adequately capture the risks to which it is exposed.

Validity of processes

88. Banks should ensure that the risk measurement methodologies are transparent to senior management, both at the bank level and within business lines, and that there are strong policies and procedures governing the circumstances under which the methodologies are changed. The risk measurement methodology should be based on sound conceptual underpinnings, and any simplifying assumptions should be based on clear and well-documented reasoning. Finally, and perhaps most significantly, the results of any operational risk measurement methodology should form an integral part of the day-to-day risk management activities of the bank, which might include: reporting to business line management, senior management and the board; performance measurement; and internal capital allocation.

89. The challenges associated with validating estimates of economic capital at a given soundness standard and risk horizon increase as one moves from market risk to credit risk to operational risk, due in large part to the decreasing availability of data across the three risk areas. In the case of operational risk, banks are experimenting with a number of techniques, both quantitative and qualitative, to increase their confidence in the reasonableness of their capital assessments.

90. In the case of statistical methodologies, inputs may include data (a bank's own internal data, pooled industry internal data, and public external data) and/or scenario-based estimates of loss frequency rates, severity rates, as well as indicators of business activity and scale. The quality of these estimates will depend largely on the comprehensiveness and relevance of the data used (discussed in previous section), in particular the coverage of the data within and across risk types and over time. Cut-off thresholds need to be reasonable in relation to the typical size of the losses associated with certain business line and event type combinations. In addition, a bank needs to ensure that its data samples and resulting parameter estimates are reflective of the range of risks it is likely to face for a given business line.

91. In the case of qualitative measures, banks should be aware that certain indicators can be interpreted in different ways. For example, staff turnover may be an indicator of either increased or reduced risk, depending on the reasons for the turnover. Similarly, greater automation may result in fewer high-frequency losses, but could increase the bank's exposure to lower-frequency, higher-severity events. For this qualitative process to be credible, banks need to have policies and procedures that govern, among other things:

- The independence of determining both the definition of the indicators to be tracked and the assessment of business lines' performance against the indicators;

- The process for changing indicators over time and validating their appropriateness and;

- The process for determining the relationship among the indicators over time.

Validity of risk estimates

92. It is also important that that the quantitative outputs of banks' risk measurement methodology are subject to validation. A potential validation technique is to compare estimates of operational risk losses with actual internal loss data. Given the low amount of available loss data for certain operational risk loss event types – as compared to the market risk area – it is difficult to apply formal statistical techniques such as backtesting and hypothesis testing. Nevertheless, banks can conduct less formal types of benchmarking and reasonableness checks of their measured loss estimates versus realized losses. Such assessments can be carried out at a number of levels, including for business lines, for risk types, and for the whole bank. For example, banks can analyse expected and realized estimates of both loss frequency and severity for any systematic or directional biases. In addition, banks may use backtesting techniques to assess the reasonableness of qualitative factors such as risk scores. Comparing the evolution of qualitative risk indicators to actual historical loss experience may shed light on the appropriate choice of certain factors and their relative weightings. In the future, as the industry begins to develop mechanisms to pool their loss experiences, banks also may be able to benchmark their parameter and loss estimates against those of industry peers. Significant deviations from the peer experience could promote a dialogue within the bank as to possible explanations for such deviations (e.g., whether it is due to potential problems with the methodology or differences in the control environment). Pooled industry loss data also could be used as a basis for validating the reasonableness of loss estimates that are based on scenario analyses of both loss frequency and severity.

93. Another quantitative technique that banks are experimenting with includes sensitivity analysis of key parameter assumptions to gauge their degree of plausibility by assessing how they behave individually and in relationship to each other. In addition, banks can perform scenario analysis and plausible stress tests of key business exposures to operational risk and compare these results to the outputs of their bank-wide measurement

methodologies. Banks could also undertake risk/return analysis by examining the implied return on economic capital numbers within business lines (summing market, credit and operational risk figures) to assess credibility of model outputs.

94. Other techniques are likely to develop over time, but it is clear that the issue of validation will require much more attention on the part of banks and supervisors as banks continue to develop their bank wide economic capital assessment methodologies.