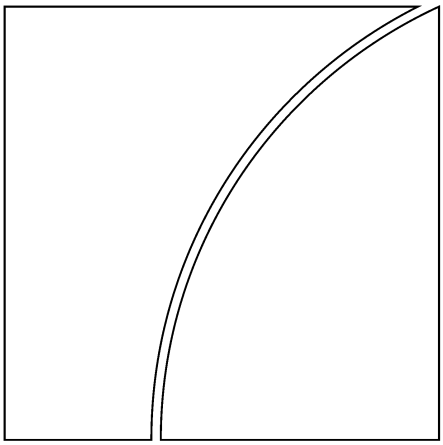
Basel Committee
on Banking Supervision



Sound Practices for the Management and Supervision of Operational Risk

July 2002

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-Kaiser
Bundesanstalt für Finanzdienstleistungsaufsicht, Bonn	Ms Kirsten Strauss
Banca d'Italia, Rome	Mr Claudio Dauria Mr Fabrizio Leandri 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	Mr Thomas Flodén
Eidgenössische Bankenkommission, Bern	Mr Martin Sprenger
Financial Services Authority, London	Mr Helmut Bauer Mr Victor Dowd Mr Jeremy Quick
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 Stephen Senior

Table of Contents

Introduction 1
Background 2
Industry Trends and Practices 3
Sound Practices 4
Developing an Appropriate Risk Management Environment 6
Risk Management: Identification, Assessment, Monitoring and Mitigation/Control 8
Role of Supervisors 12
Role of Disclosure 14

Sound Practices for the Management and Supervision of Operational Risk

The consultative paper Sound Practices for the Management and Supervision of Operational Risk, prepared by the Risk Management Group of the Basel Committee on Banking Supervision (the Committee), was originally published in December 2001. The Committee is grateful for the many insightful comments received from institutions, industry associations, supervisory authorities, and others, and notes that these comments have played a substantial role in the redrafting of this paper. Due to a number of important changes to the Sound Practices incorporated in this revised draft, the Committee has decided to release the paper for a second, short period of consultation before finalisation.[1] The Committee would therefore welcome comments on the revised principles outlined in this paper. These comments 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 30 September 2002. Comments may be submitted via e-mail: BCBS.capital@bis.org[2] or by fax: + 41 61 280 9100. Comments on this paper will not be posted on the BIS website.

Introduction

1. The following paper outlines a set of principles that provide a framework for the effective management and supervision of operational risk, for use by banks and supervisory authorities when evaluating operational risk management policies and practices.

2. The Committee recognises that the exact approach for operational risk management 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. However, despite these differences, clear strategies and oversight by the board of directors and senior management, a strong internal control culture (including, among other things, clear lines of responsibility and segregation of duties), effective internal reporting, and contingency planning are all crucial elements of an effective operational risk management framework 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.

---

[1] Please note that the Committee does not plan to issue a revised version of the second part of the December 2001 Sound Practices paper *Supervisory Guidance for a Comprehensive Operational Risk Management Programme*.

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

Background

3. 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 suggest that risks other than credit, interest rate risk and market risk can be substantial. Examples of these new and growing risks faced by banks include:

- If 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;
- 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, netting arrangements and asset securitisations) to optimise their exposure to market risk and credit risk, but which in turn may produce other forms of risk; and
- Growing use of outsourcing arrangements and the participation in clearing and settlement systems can mitigate some risk but can also present significant other risks to banks.

4. The diverse set of risks listed above can be grouped under the heading of 'operational risk', which for supervisory purposes the Committee has defined as: 'the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events'.[3] The definition includes legal risk but excludes strategic, reputational and systemic risk.

5. The Committee recognises that operational risk is a term that has a variety of meanings within the industry, and therefore for internal purposes, banks may choose to adopt their own definitions of operational risk. Whatever the exact definition, a clear understanding by banks of what is meant by operational risk is critical to the effective management and control of this risk category. It is also important that the definition considers the full range of material operational risks facing the bank and captures the most significant causes of severe operational losses. Operational risk event types that the Committee - in co-operation with the industry - has identified as having the potential to result in substantial losses include the following:

- ***Internal fraud.*** Acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involve at least one internal party. Examples include intentional

[3] This definition was adopted from the industry as part of the Committee's work in developing a minimum regulatory capital charge for operational risk. While this paper is not a formal part of the capital framework, the Committee nevertheless expects that the basic elements of a sound operational risk management framework set out in this paper will inform supervisory expectations when reviewing bank capital adequacy.

misreporting of positions, employee theft, and insider trading on an employee's own account.

- ***External fraud.*** Acts by a third party, of a type intended to defraud, misappropriate property or circumvent the law. Examples include robbery, forgery, cheque kiting, and damage from computer hacking.

- ***Employment practices and workplace safety.*** Acts inconsistent with employment, health or safety laws or agreements, or which result in payment of personal injury claims, or claims relating to diversity/discrimination issues. Examples include workers compensation claims, violation of employee health and safety rules, organised labour activities, discrimination claims, and general liability (for example, a customer slipping and falling at a branch office).

- ***Clients, products and business practices.*** Unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product. Examples include fiduciary breaches, misuse of confidential customer information, improper trading activities on the bank's account, money laundering, and sale of unauthorised products.

- ***Damage to physical assets.*** Loss or damage to physical assets from natural disaster or other events. Examples include terrorism, vandalism, earthquakes, fires and floods.

- ***Business disruption and system failures.*** Disruption of business or system failures. Examples include hardware and software failures, telecommunication problems, and utility outages.

- ***Execution, delivery and process management.*** Failed transaction processing or process management, and relations with trade counterparties and vendors. Examples include data entry errors, collateral management failures, incomplete legal documentation, unapproved access given to client accounts, non-client counterparty misperformance, and vendor disputes.

Industry Trends and Practices

6. 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 have involved numerous meetings with banking organisations, surveys of industry practice, and analyses of the results. Based upon these efforts, the Committee believes that it has a good understanding of the banking industry's current range of practices, as well as the industry's efforts to develop methods for managing operational risks.

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

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

9. This paper is organised along the following lines: developing an appropriate risk management environment; risk management: identification, assessment, monitoring and control/mitigation; the role of supervisors; and the role of disclosure.

Sound Practices

10. In developing these sound practices, the Committee has drawn upon its existing work on the management of other significant banking risks, such as credit risk, interest rate risk and liquidity risk, and the Committee believes that similar rigour should be applied to the management 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 affects the risk management process.[4] At the same time, failure to properly manage operational risk can result in a misstatement of an institution's risk/return profile and expose the institution to significant losses. Reflecting the different nature of operational risk, for the purposes of this paper, 'management' of operational risk is taken to mean the 'identification, assessment, monitoring and control/mitigation' of risk. This definition contrasts with the one used by the Committee in previous risk management papers of the 'identification, measurement, monitoring and control' of risk. In common with its work on other banking risks, the Committee has structured this sound practice paper around a number of principles. These are:

Developing an Appropriate Risk Management Environment

Principle 1: The board of directors[5] should be aware of the major aspects of the bank's operational risks as a distinct risk category that should be managed, and it should

---

[4] However, the Committee recognises that in some business lines with minimal credit or market risk (e.g., asset management, and payment and settlement), the decision to incur operational risk, or compete based on the ability to manage and effectively price this risk, is an integral part of a bank's risk/reward calculus.

[5] 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, 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 terms '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.

approve and periodically review the bank's operational risk management framework. The framework should provide a firm-wide definition of operational risk and lay down the principles of how operational risk is to be identified, assessed, monitored, and controlled/mitigated.

Principle 2: The board of directors should ensure that the bank's operational risk management framework is subject to effective and comprehensive internal audit by operationally independent, appropriately trained and competent staff. The internal audit function should not be directly responsible for operational risk management.

Principle 3: Senior management should have responsibility for implementing the operational risk management framework approved by the board of directors. The framework should be implemented 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.

Risk Management: Identification, Assessment, Monitoring, and Mitigation/Control

Principle 4: Banks should identify and assess the operational risk inherent in all material 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 implement a process to regularly monitor operational risk profiles and material exposure to losses. There should be regular reporting of pertinent information to senior management and the board of directors that supports the proactive management of operational risk.

Principle 6: Banks should have policies, processes and procedures to control or mitigate material operational risks. Banks should assess the feasibility of alternative risk limitation and control strategies and should adjust their operational risk profile using appropriate strategies, in light of their overall risk appetite and profile.

Principle 7: Banks should have in place contingency and business continuity plans to ensure their ability to operate as going concerns and minimise losses in the event of severe business disruption.

Role of Supervisors

Principle 8: Banking supervisors should require that all banks, regardless of size, have an effective framework in place to identify, assess, monitor and control or mitigate material 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 policies, procedures and practices related to operational risks. Supervisors should ensure that there are appropriate 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 approach to operational risk management.

Developing an Appropriate Risk Management Environment

11. Failure to understand and manage 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. Both the board and senior management are responsible for creating an organisational culture that places a high priority on effective operational risk management and adherence to sound operating controls. Operational risk management is most effective where a bank's culture emphasises high standards of ethical behaviour at all levels of the bank. The board and senior management should promote an organisational culture which establishes through both actions and words the expectations of integrity for all employees in conducting the business of the bank.

Principle 1: The board of directors should be aware of the major aspects of the bank's operational risks as a distinct risk category that should be managed, and it should approve and periodically review the bank's operational risk management framework. The framework should provide a firm-wide definition of operational risk and lay down the principles of how operational risk is to be identified, assessed, monitored, and controlled/mitigated.

12. The board of directors should approve the implementation of a firm-wide framework to explicitly manage operational risk as a distinct risk to the bank's safety and soundness. The board should provide senior management with clear guidance and direction regarding the principles underlying the framework and approve the corresponding policies developed by senior management.

13. In this paper, an operational risk framework is understood to include an appropriate definition of operational risk which clearly articulates what constitutes operational risk in that bank. The framework should cover the bank's appetite and tolerance for operational risk, as specified through the policies for managing this risk, including the extent of, and manner in which, operational risk is transferred outside the bank. It should also include policies outlining the bank's approach to identifying, assessing, monitoring and controlling/mitigating the risk. The formality and sophistication of the bank's operational risk management framework should be commensurate with the risk incurred by the bank.

14. The board is responsible for establishing a management structure capable of implementing the firm's operational risk management framework. Since a significant aspect of managing operational risk relates to the establishment of strong internal controls, it is particularly important that the board establish clear lines of management responsibility, accountability and reporting. In addition, there must be segregated responsibilities and reporting lines between control functions and the revenue generating business lines. The framework should also articulate the key processes the firm needs to have in place to manage operational risk.

15. The board should review the framework 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 appropriate for the bank's activities, systems and processes. If necessary, the board should ensure that the operational risk management framework is revised in light of this analysis, so that material operational risks are captured within the framework.

Principle 2: The board of directors should ensure that the bank's operational risk management framework is subject to effective and comprehensive internal audit by

operationally independent, appropriately trained and competent staff. The internal audit function should not be directly responsible for operational risk management.

16. Banks should have in place adequate internal audit coverage to verify that operating policies and procedures are effectively implemented.[6] 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. Audit should periodically validate that the firm's operational risk management framework is being implemented effectively across the firm.

17. To the extent that the audit function is involved in oversight of the operational risk management framework, 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. The audit function may provide valuable input to those responsible for operational risk management, but should not itself have direct operational risk management responsibilities. In practice, the Committee recognises that the audit function at some banks (particularly smaller banks) may have initial responsibility for developing an operational risk management programme. Where this is the case, banks should see that responsibility for day-to-day operational risk management is transferred elsewhere in a timely manner.

Principle 3: Senior management should have responsibility for implementing the operational risk management framework approved by the board of directors. The framework should be implemented 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 framework established by the board of directors into more specific policies, processes and procedures that can be implemented and verified within different business units. 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 unit's policy 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 policy have authority independent from the business units they oversee. Management should ensure that the bank's operational risk management policy has been clearly communicated to staff at all levels in business units that incur material operational risks.

20. Senior management should ensure that staff with responsibility for operational risk communicate effectively with staff responsible for credit, market, and other risks, as well as

---

[6] 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.

with those in the firm who are responsible for the procurement of external services such as insurance purchasing and outsourcing agreements. Failure to do so may result in significant gaps or overlaps in a bank's overall risk management programme.

21. Senior management should also ensure that the bank's remuneration policies are consistent with its appetite for risk. Remuneration policies that reward staff that deviate from policies (e.g. by exceeding established limits) weaken the bank's risk management processes.

22. 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.

Risk Management: Identification, Assessment, Monitoring and Mitigation/Control

Principle 4: Banks should identify and assess the operational risk inherent in all material 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.

23. Risk identification is paramount for the subsequent development of viable operational 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 changes in the industry and technological advances) that could adversely affect the achievement of the bank's objectives.

24. In addition to identifying the most potentially adverse risks, banks should assess their vulnerability to these risks. Effective risk assessment allows the bank to better understand its risk profile and most effectively target risk management resources.

25. There are several processes commonly used by banks to help them identify and assess operational risk:

- Self- or Risk Assessment: a bank assesses its operations and activities against a menu of potential operational risk vulnerabilities. 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 tend to be reviewed on a periodic basis (such as monthly or quarterly) to alert banks to changes that may be indicative of risk concerns. Such indicators may include the number of failed trades, staff turnover rates and the frequency and/or severity of errors and omissions.

- Scorecards: these provide a means of translating qualitative assessments into quantitative metrics that give a relative ranking of different types of operational risk

exposures. Some scores may relate to risks unique to a specific business line while others may rank risks that cut across business lines. Scores may address factors inherent risks, as well as the controls to mitigate them. In addition, scorecards may be used to allocate economic capital to business lines in relation to performance in managing and controlling various aspects of operational risk.

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

- Measurement: some firms have begun to quantify their exposure to operational risk using a variety of approaches. For example, data on a bank's historical loss experience could provide meaningful information for assessing the bank's exposure to operational risk and developing a policy to mitigate/control the risk. An effective way of making good use of this information is to establish a framework for systemically tracking and recording the frequency, severity and other relevant information on individual loss events. Some firms have also combined internal loss data with external loss data, scenario analyses, and qualitative assessment factors.

Principle 5: Banks should implement a process to regularly monitor operational risk profiles and material exposure to losses. There should be regular reporting of pertinent information to senior management and the board of directors that supports the proactive management of operational risk.

26. An effective monitoring process is essential for adequately managing operational risk. Regular 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 frequency and/or severity of a loss event.

27. In addition to monitoring operational loss events, banks should identify indicators that may be predictive of the risk of future losses. Such indicators (often referred to as key risk indicators or early warning indicators) should be forward-looking and could reflect potential sources of operational risk such as rapid growth, the introduction of new products, employee turnover, transaction breaks, system downtime, etc. When thresholds are directly linked to these indicators an effective monitoring process can help identify key material risks in a transparent manner and enable the bank to act upon these risks appropriately.

28. 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. Reports generated by supervisory authorities may also inform this monitoring and should likewise be reported internally to senior management and the board, where appropriate.

29. 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 to areas of the bank on which areas of concern may have an impact. Reports should fully reflect 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.

30. In general, the board of directors should receive sufficient higher-level information to enable them to understand the bank's overall risk profile and focus on the material and strategic implications of operational risk to the business.

Principle 6: Banks should have policies, processes and procedures to control or mitigate material operational risks. Banks should assess the feasibility of alternative risk limitation and control strategies and should adjust their operational risk profile using appropriate strategies, in light of their overall risk appetite and profile.

31. Control activities are designed to address the risks that a bank has identified.[7] For those risks that are controllable, the bank must decide to what extent it wishes to use control procedures and other appropriate techniques, or bear the risk. For those risk that cannot be controlled, the bank must decide whether to accept these risk 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. Principle 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. Although a framework of formal, written policies and procedures is critical, it needs to be reinforced through a strong control culture that promotes sound risk management practices. To be effective, control activities should be an integral part of the regular activities of a bank. 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. In addition to segregation of duties, banks should ensure that a number of other internal practices are in place to control operational risk. Among these are close monitoring of adherence to assigned risk limits or thresholds, maintaining safeguards for access to and

[7] For more detail, see the *Framework for Internal Control Systems in Banking Organisations*, Basel Committee on Banking Supervision, September 1998.

use of bank assets and records, ensuring that staff has appropriate expertise and training, identifying business lines or products where returns appear to be significantly out of line with reasonable expectations, and regular verification and reconciliation of transactions and accounts. Failure to implement such practices has resulted in significant operational losses for some banks in recent years.

35. The Committee has observed that operational risk appears to be prevalent where banks have engaged in new activities or developed new products (particularly where these activities or products are not consistent with the bank's core business strategies), entered unfamiliar markets, and engaged in businesses that are geographically distant from the head office. Moreover, in many such instances, the firm did not ensure that the risk management control infrastructure kept pace with the growth in the new business activity. A number of the most sizeable and highest-profile losses that have occurred in recent years have taken place where one or a combination of these conditions existed. Therefore, it is incumbent upon banks to ensure that special attention is paid to internal control activities where such conditions exist.

36. Some significant operational risks have low probabilities but potentially very large financial impact. Moreover, not all risk events can be controlled (e.g., natural disasters). Risk mitigation tools or programmes can be used to reduce the exposure to, or frequency and/or severity of, such events. For example, insurance policies, particularly those with prompt and certain pay-out features, can be used to externalise the risk of "low frequency, high severity" losses which may occur as a result of events such as third-party claims resulting from errors and omissions, physical loss of securities, employee or third-party fraud, and natural disasters.

37. However, banks should view risk mitigation tools as complementary to, rather than a replacement for, thorough internal operational risk control. 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 the extent to which risk mitigation tools such as insurance truly reduce risk, or transfer the risk to another business sector or area, or even create a new risk.

38. Investments in appropriate processing technology and information technology security are also important for risk mitigation. However, banks should be aware that increased automation could 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. As discussed below in Principle 7, banks should establish business resumption and contingency plans that address this risk.

39. Banks should also establish sound policies for managing the risks associated with outsourcing activities. Outsourcing of activities 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. However, a bank's use of third parties does not diminish the responsibility of the board of directors and management to ensure that the third-party activity is conducted in a safe and sound manner and in compliance with applicable laws. Outsourcing activities should be based on rigorous legal agreements ensuring a clear allocation of responsibilities between external service providers and the outsourcing bank. Furthermore, banks need to manage any residual risks associated with outsourcing arrangements, including disruption of services or reputational risks.

40. 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 or intra-group service providers, including both operational breakdowns and the potential business failure or default of the external parties. The board and management should ensure that the expectations and obligations of each party are clearly defined, understood and enforceable. 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.

41. In some instances, banks may decide to either retain a certain level of operational risk or self-insure against that risk. Where this is the case and the risk is material, the decision to retain or self-insure the risk should be transparent within the organisation and should be consistent with the bank's overall business strategy and appetite for risk.

Principle 7: Banks should have in place contingency and business continuity plans to ensure their ability to operate as going concerns and minimise losses in the event of severe business disruption.

42. For reasons that may be beyond a bank's control, a severe event may result in the inability of the bank to fulfil some or all of its business obligations, particularly where the bank's physical, telecommunication, or information technology infrastructures have been damaged or made inaccessible. This can, in turn, result in significant financial losses to the bank, as well as broader disruptions to the financial system through channels such as the payments system. This potential requires that banks establish business resumption and contingency plans that take into account different types of plausible scenarios to which the bank may be vulnerable, commensurate with the size and complexity of the bank's operations.

43. Banks should identify critical business processes, including those where there is dependence on external vendors or other third parties, for which rapid resumption of service would be most essential. For these processes, banks should identify alternative mechanisms for resuming service in the event of an outage. Particular attention should be paid to the ability to restore electronic or physical records that are necessary for business resumption. Where such records are backed-up at an off-site facility, or where a bank's operations must be relocated to a new site, care should be taken that these sites are at an adequate distance from the impacted operations to minimise the risk that both primary and back-up records and facilities will be unavailable simultaneously.

44. Banks should periodically review their business resumption and contingency plans so that they are consistent with the bank's current operations and business strategies. Moreover, these plans should be tested periodically to ensure that the bank will be able to execute the plans in the unlikely event of a severe business disruption.

Role of Supervisors

Principle 8: Banking supervisors should require that all banks, regardless of size, have an effective framework in place to identify, assess, monitor and control or mitigate material operational risks as part of an overall approach to risk management.

45. To the extent that operational risks pose a threat to banks' safety and soundness, supervisors have a responsibility to encourage banks to develop and use better techniques in managing those risks. Consequently, supervisors should require banks to develop operational risk management frameworks consistent with the guidance in this paper and commensurate with their size, complexity, and risk profiles.

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

46. The independent evaluation of operational risk by supervisors 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, if appropriate, its internal capital targets;
- The effectiveness of the bank's risk management process and overall control environment with respect to operational risk;
- The bank's systems for monitoring and reporting its operational risk profile, including data on operational losses and other indicators of potential operational risk;
- The bank's procedures for the timely and effective resolution of operational risk events and vulnerabilities;
- The bank's process of internal controls, reviews and audit to ensure the integrity of the overall operational risk management process;
- The effectiveness of the bank's operational risk mitigation efforts; and
- The quality and comprehensiveness of the bank's business resumption and contingency plans.

47. 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 an appropriate and integrated manner across the group. In performing this assessment, co-operation and exchange of information with other supervisors, in accordance with established procedures, may be necessary. Some supervisors may choose to use external auditors in these assessment processes.

48. 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.

49. Given the general recognition that comprehensive operational risk management processes are still in development at many banks, supervisors should take an active role in encouraging ongoing internal development efforts by monitoring 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 ensure effective business line management of operational risk, to provide clear lines of communication and responsibility, and to encourage active self assessment of existing practices and consideration of possible risk mitigation enhancements.

Role of Disclosure

Principle 10: Banks should make sufficient public disclosure to allow market participants to assess their approach to operational risk management.

50. The Committee believes that the timely and frequent public disclosure of relevant information by banks can lead to enhanced market discipline and, therefore, more effective risk management. The amount of disclosure should be commensurate with the size and complexity of a bank's operations, as well as market demand for such information.

51. The area of operational risk disclosure is not yet well established, primarily because banks are still in the process of developing operational risk assessment techniques. However, the Committee believes that a bank should disclose its operational risk management framework in a manner that will allow investors and counterparties to determine whether a bank effectively identifies, assesses, monitors and controls operational risk.