FRAMEWORK

FOR THE EVALUATION OF

INTERNAL CONTROL SYSTEMS

Basle Committee on Banking Supervision

Basle

January 1998

Table of contents

	Page
Introduction	1
I. Background	6
II. The objectives and role of the internal controls framework	8
III. The major elements of an internal control process	
A. Management oversight and the control culture	10
1. Board of directors	10
2. Senior management	11
3. Control culture	12
B. Risk assessment	13
C. Control activities	14
D. Information and communication	16
E. Monitoring	18
IV. Evaluation of internal control systems by supervisory	21
V. Role and responsibilities of external auditors	24
Appendix - Supervisory lessons learned from internal control	25

Framework for the Evaluation of Internal Control Systems

INTRODUCTION

1. As part of its on-going efforts to address bank supervisory issues and enhance supervision through guidance that encourages sound risk management practices, the Basle Committee on Banking Supervision[1] is issuing this draft framework for comment by bank supervisors and other interested parties. It is intended that this framework will be used by supervisors in evaluating banks' internal control systems. A system of effective internal controls is a critical component of bank management and a foundation for the safe and sound operation of banking organisations. A system of strong internal controls can help to ensure that the goals and objectives of a banking organisation will be met, that the bank will achieve long-term profitability targets, and maintain reliable financial and managerial reporting. Such a system can also help to ensure that the bank will comply with laws and regulations as well as policies, plans, internal rules and procedures, and decrease the risk of unexpected losses or damage to the bank's reputation. The paper describes the essential elements of a sound internal control system, drawing upon experience in member countries and principles established in earlier publications by the Committee. The objective of the paper is to outline a number of principles for use by supervisory authorities when evaluating banks' internal control systems.

2. The Basle Committee, along with banking supervisors throughout the world, has focused increasingly on the importance of sound internal controls. This heightened interest in internal controls is, in part, a result of significant losses incurred by several banking organisations. An analysis of the problems related to these losses indicates that they could probably have been avoided had the banks maintained effective internal control systems. Such systems would have prevented or enabled earlier detection of the problems that led to the losses, thereby limiting damage to the banking organisation. In developing these principles, the Committee has drawn on lessons learned from problem bank situations in individual member countries.

3. These principles are intended to be of general application and supervisory authorities should use them in assessing their own supervisory methods and procedures for

---

1 The Basle Committee on Banking Supervision is a Committee of banking supervisory authorities which was established by the central-bank Governors of the Group of Ten countries in 1975. It consists of senior representatives of bank supervisory authorities and central banks from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, Netherlands, Sweden, Switzerland, United Kingdom and the United States. It usually meets at the Bank for International Settlements in Basle, where its permanent Secretariat is located.

monitoring how banks structure their internal control systems. While the exact approach chosen by individual supervisors will depend upon a host of factors, including their on-site and off-site supervisory techniques and the degree to which external auditors are also used in the supervisory function, **all members of the Basle Committee agree that the principles set out in this paper should be used in evaluating a bank's internal control system.**

4. The Basle Committee is distributing this paper to supervisory authorities worldwide in the belief that the principles presented will provide a useful framework for the effective supervision of internal control systems. More generally, the Committee wishes to emphasise that sound internal controls are essential to the prudent operation of banks and to promoting stability in the financial system as a whole.

5. The guidance previously issued by the Basle Committee typically included discussions of internal controls affecting specific areas of bank activities, such as interest rate risk, and trading and derivatives activities. In contrast, this guidance presents a framework that the Basle Committee encourages supervisors to use in evaluating the internal controls over all on- and off-balance sheet activities of banking organisations. The guidance does not focus on specific areas or activities within a banking organisation. The exact application depends on the nature, complexity and risks of the bank's operations. The Committee stipulates in sections III and IV of the paper fourteen principles for banking supervisory authorities to apply in assessing banks' internal control systems. In addition, the Appendix provides supervisory lessons learned from past internal control failures.

Principles for the Assessment of Internal Control Systems

Management oversight and the control culture

Principle 1:

The board of directors should have responsibility for approving strategies and policies; understanding the risks run by the bank, setting acceptable levels for these risks and ensuring that senior management takes the steps necessary to identify, monitor and control these risks; approving the organisational structure; and ensuring that senior management is monitoring the effectiveness of the internal control system.

Principle 2:

Senior management should have responsibility for implementing strategies approved by the board; setting appropriate internal control policies; and monitoring the effectiveness of the internal control system.

Principle 3:

The board of directors and senior management are responsible for promoting high ethical and integrity standards, and for establishing a culture within the organisation that emphasises and demonstrates to all levels of personnel the importance of internal controls. All levels of personnel at a banking organisation need to understand their role in the internal controls process and be fully engaged in the process.

Risk Assessment

Principle 4:

Senior management should ensure that the internal and external factors that could adversely affect the achievement of the bank's objectives are being identified and evaluated. This assessment should cover all the various risks facing the bank (for example, credit risk, country and transfer risk, market risk, interest rate risk, liquidity risk, operational risk, legal risk and reputational risk).

Principle 5:

Senior management should ensure that the risks affecting the achievement of the bank's strategies and objectives are continually being evaluated. Internal controls may need to be revised to appropriately address any new or previously uncontrolled risks.

Control Activities

Principle 6:

Control activities should be an integral part of the daily operations of a bank. Senior management must set up an appropriate control structure to ensure effective internal controls, defining the control activities at every business level. These should include: top level reviews; appropriate activity controls for different departments or divisions; physical controls; periodic checking for compliance with exposure limits; a system of approvals and authorisations; and, a system of verification and reconciliation. Senior management must periodically ensure that all areas of the bank are in compliance with established policies and procedures.

Principle 7:
Senior management should ensure that there is appropriate segregation of duties and that personnel are not assigned conflicting responsibilities. Areas of potential conflicts of interest should be identified, minimised, and carefully monitored.

Information and communication

Principle 8:
Senior management should ensure that there are adequate and comprehensive internal financial, operational and compliance data, as well as external market information about events and conditions that are relevant to decision making. Information should be reliable, timely, accessible, and provided in a consistent format.

Principle 9:
Senior management should establish effective channels of communication to ensure that all staff are fully aware of policies and procedures affecting their duties and responsibilities and that other relevant information is reaching the appropriate personnel.

Principle 10:
Senior management must ensure that there are appropriate information systems in place that cover all activities of the bank. These systems, including those that hold and use data in an electronic form, must be secure and periodically tested.

Monitoring

Principle 11:
Senior management should continually monitor the overall effectiveness of the bank's internal controls in helping to achieve the organisation's objectives. Monitoring of key risks should be part of the daily operations of the bank and should include separate evaluations as required.

Principle 12:
There should be an effective and comprehensive internal audit of the internal control system carried out by appropriately trained and competent staff. The internal audit function, as part of the monitoring of the system of internal controls, should report directly to the board of directors or its audit committee, and to senior management.

Principle 13:

Identified internal control deficiencies should be reported in a timely manner to the appropriate management level and addressed promptly. Material internal control deficiencies should be reported to senior management and the board of directors.

Evaluation of Internal Control Systems by Supervisory Authorities

Principle 14:

Supervisors should require that all banks, regardless of size, have an effective system of internal controls that is consistent with the nature, complexity, and risk of their on- and off-balance-sheet activities and that responds to changes in the bank's environment and conditions. In those instances where supervisors determine that a bank's internal control system is not adequate (for example, does not cover all of the principles contained in this document), they should take action against the bank to ensure that the internal control system is improved immediately.

6. Comment is invited on all aspects of this paper, including the Appendix, by 30th March 1998.

I. Background

1. The Basle Committee has been studying recent banking problems in order to identify the major sources of internal control problems. The problems identified reinforce the importance of having bank directors and management, internal and external auditors, and bank supervisors focus considerable attention on strengthening internal control systems and continually evaluating their effectiveness. Several recent cases demonstrate that lax internal controls can lead to significant losses for banks.

2. The types of control breakdowns typically seen in problem bank cases can be grouped into five broad categories:

- ***Lack of adequate management oversight and accountability, and failure to develop a strong control culture within the bank.*** Without exception, cases of major loss reflect management inattention to, and laxity in, the control culture of the bank, insufficient guidance and oversight by boards of directors and senior management, and a lack of clear management accountability through the assignment of roles and responsibilities. These cases also reflect insufficient incentives to carry out strong line supervision and maintain a high level of control consciousness within business areas.
- ***Inadequate assessment of the risk of certain banking activities, whether on- or off-balance sheet.*** Many banking organisations that have suffered major losses neglected to continually assess the risks of new products and activities, or update their risk assessments when significant changes occurred in the environment or business conditions. Many recent cases highlight the fact that control systems that function well for traditional or simple products are unable to handle more sophisticated or complex products.
- ***The absence or failure of key control activities, such as segregation of duties, approvals, verifications, reconciliations, and reviews of operating performance.*** Lack of segregation of duties in particular has played a major role in the significant losses that have occurred at banks.
- ***Inadequate communication of information between levels of management within the bank, especially in the upward communication of problems.*** To be effective, policies and procedures need to be effectively communicated to all personnel involved in an activity. Some losses in banks occurred because relevant personnel were not aware of or did not understand the bank's policies. In several instances, information about inappropriate activities that should have been reported upward through organisational levels was not communicated to the board of directors or senior management until the problems became severe. In other instances, information in management reports was not complete or accurate, creating a favourable impression of a business situation that was in fact problematic.

- ***Inadequate or ineffective audit programs and other monitoring activities.*** In many cases, audits were not sufficiently rigorous to identify and report the control weaknesses associated with problem banks. In other cases, even though auditors reported problems, they were not corrected by management.

3. The internal control framework underlying this guidance is based on practices currently in place at many major banks, securities firms, and non-financial companies, and their auditors. Moreover, this evaluation framework is consistent with the increased emphasis of banking supervisors on the review of a banking organisation's risk management and internal control processes. It is important to emphasise that it is the responsibility of a bank's board of directors and senior management to ensure that adequate internal controls are in place at the bank and to foster an environment where individuals understand and take seriously their responsibilities in this area. In turn, it is the responsibility of banking supervisors to assess the commitment of a bank's board of directors and management to the internal control process.

II. The Objectives and Role of the Internal Control Framework

4. Internal control is a *process* effected by the board of directors,[2] senior management and all levels of personnel. It is not solely a procedure or policy that is performed at a certain point in time, but rather it is continually operating at all levels within the bank. The board of directors and senior management are responsible for establishing the appropriate culture to facilitate an effective internal control process and for continuously monitoring its effectiveness; however, each individual within an organisation must participate in the process. The main objectives of the internal control process can be categorised as follows:[3]

1. efficiency and effectiveness of operations (operational objectives);
2. reliability and completeness of financial and management information (information objectives); and
3. compliance with applicable laws and regulations (compliance objectives).

5. *Operational objectives* for internal control pertain to the effectiveness and efficiency of the bank in using its assets and other resources and protecting the bank from loss. The internal control process seeks to ensure that personnel throughout the organisation are working to achieve its objectives in a straightforward manner, without unintended or excessive cost or placing other interests (such as an employee's, vendor's or customer's interest) before those of the bank.

6. *Information objectives* address the preparation of timely, reliable reports needed for decision-making within the banking organisation. They also address the need for reliable annual accounts, other financial statements and other financial-related disclosures, including those for regulatory reporting and other external uses. The information received by management, the board of directors, shareholders and supervisors should be of sufficient quality and integrity that recipients can rely on the information in making decisions. The term reliable, as it relates to financial statements, refers to the preparation of statements that are

---

[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.

[3] These include internal controls over safeguarding of assets and other resources against unauthorised acquisition, use or disposition, or loss.

presented fairly and based on comprehensive and well-defined accounting principles and rules.

7. *Compliance objectives* ensure that all banking business is conducted in compliance with applicable laws and regulations, supervisory requirements, and internal policies and procedures. This objective must be met in order to protect the bank's franchise and reputation.

III. The Major Elements of an Internal Control Process

8. The internal control process, which historically has been a mechanism for reducing instances of fraud, misappropriation and errors, has recently become more extensive, addressing all the various risks faced by banking organisations. It is now recognised that a sound internal control process is critical to a bank's ability to meet its established goals and objectives, and to maintain its financial viability.

9. Internal control consists of five interrelated elements:

1. management oversight and the control culture;
2. risk assessment;
3. control activities;
4. information and communication; and
5. monitoring activities.

The problems observed in recent large losses at banks can be aligned with these five elements. The effective functioning of these elements is essential to achieving a bank's operational, information, and compliance objectives.

A. Management Oversight and the Control Culture

1. Board of directors

Principle 1: The board of directors should have responsibility for approving strategies and policies; understanding the risks run by the bank, setting acceptable levels for these risks and ensuring that senior management takes the steps necessary to identify, monitor and control these risks; approving the organisational structure; and ensuring that senior management is monitoring the effectiveness of the internal control system.

10. The board of directors provides governance, guidance and oversight to senior management. It is responsible for setting the broad strategies and major policies of the organisation and approving the overall organisational structure. The board of directors has the ultimate responsibility for ensuring that an adequate system of internal controls is established and maintained. Effective board members are objective, capable, and inquisitive, with a knowledge of the activities of and risks run by the bank. A strong, active board, particularly when coupled with effective upward communication channels and capable financial, legal, and internal audit functions, is often best able to ensure the correction of problems that may diminish the effectiveness of the internal control system.

11. The board of directors should include in its activities (1) periodic discussions with management concerning the effectiveness of the internal control system, (2) a timely review of evaluations of internal controls made by management, internal auditors, and external auditors, and (3) periodic efforts to ensure that management has appropriately followed up on

recommendations and concerns expressed by auditors and supervisory authorities on internal control weaknesses.

12. One option used by banks in many countries is the establishment of an independent audit committee to assist the board in carrying out its responsibilities. The establishment of an audit committee allows for detailed examination of information and reports without the need to take up the time of all directors and ensures that the particular questions concerned receive proper attention. The audit committee is typically responsible for overseeing the financial reporting process and the internal control system. As part of this responsibility, the audit committee typically oversees the operations of, and serves as a direct contact for, the bank's internal audit department and engages and serves as the primary contact for the external auditors. In those countries where it is an option, the committee should be composed entirely of outside directors (i.e., members of the board that are not employed by the bank or any of its affiliates) who have knowledge of financial reporting and internal controls. It should be noted that in no case should the creation of an audit committee amount to a transfer of duties away from the full board, which alone is legally empowered to take decisions.

2. Senior management

Principle 2: Senior management should have responsibility for implementing strategies approved by the board; setting appropriate internal control policies; and monitoring the effectiveness of the internal control system.

13. Senior management is responsible for carrying out directives approved by the board of directors, including the implementation of strategies and policies and the establishment of an effective system of internal control. Members of senior management typically delegate responsibility for establishing more specific internal control policies and procedures to those responsible for a particular unit's activities or functions. Consequently, it is important for senior management to ensure that the managers to whom they have delegated these responsibilities develop and enforce appropriate policies and procedures.

14. Compliance with an established internal control system is heavily dependent on a well-documented and communicated organisational structure that clearly shows lines of reporting responsibility and authority and provides for effective communication throughout the organisation. The allocation of duties and responsibilities should ensure that there are no gaps in reporting lines and that an effective level of management control is extended to all levels of the bank and its various activities.

15. It is important that senior management takes steps to ensure that activities are conducted by qualified staff with the necessary experience and technical capabilities. Staff should be properly compensated and their training and skills periodically updated. Senior

management should institute compensation and promotion policies that reward appropriate behaviours and minimise incentives for staff to ignore or override internal control mechanisms.

3. Control culture

Principle 3: The board of directors and senior management are responsible for promoting high ethical and integrity standards, and for establishing a culture within the organisation that emphasises and demonstrates to all levels of personnel the importance of internal controls. All levels of personnel at a banking organisation need to understand their role in the internal controls process and be fully engaged in the process.

16. An essential element of an effective system of internal control is a strong control culture. It is the responsibility of the board of directors and senior management to emphasise the importance of internal control through their actions and words. This includes the ethical values management displays in their business dealings, both inside and outside the organisation. The words, attitudes and actions of the board of directors and senior management affect the integrity, ethics and other aspects of the bank's control culture.

17. In varying degrees, internal control is the responsibility of everyone in a bank. Almost all employees produce information used in the internal control system or take other actions needed to effect control. An essential element of a strong internal control system is the recognition by every employee of the need to carry out their responsibilities effectively and to communicate to the appropriate level of management any problems in operations, instances of non-compliance with the code of conduct, or other policy violations or illegal actions that are noticed. This can best be achieved when operational procedures are contained in clearly written documentation that is made available to all relevant personnel. It is essential that all personnel within the bank understand the importance of internal control and are actively engaged in the process.

18. In reinforcing ethical values, banking organisations should avoid policies and practices that may inadvertently provide incentives or temptations for inappropriate activities. Examples of such policies and practices include undue emphasis on performance targets or other operational results, particularly short term ones; high performance-dependent compensation rewards; ineffective segregation of duties or other controls that may offer temptations to misuse resources or conceal poor performance; and insignificant or overly onerous penalties for improper behaviours.

19. While having a strong internal control culture does not guarantee that an organisation will reach its goals, the lack of such a culture provides greater opportunities for errors to go undetected or for improprieties to occur.

B. Risk Assessment

20. From an internal control perspective, a risk assessment should identify and evaluate the internal and external factors that could adversely affect the achievement of the banking organisation's operational, information and compliance objectives. This should cover such risks as credit, market, liquidity and operational risk (which includes the risk of fraud, misappropriation of assets, and unreliable financial information). There is a significant difference between risk assessment in the context of the internal control process and the broader concept of the "risk management" of a bank's overall business. For example, the risk management process in a banking organisation consists of setting organisational goals and objectives (such as profitability targets) and identifying, measuring and setting limits on the risk exposures that the bank will accept in order to achieve its objectives. The internal control process then works to ensure that objectives and policies are communicated and implemented, that compliance with limits is monitored, and that deviations are corrected in accordance with management's policies. Thus, the concept of risk management includes, but is not limited to, both risk assessment and the setting of operational objectives as those terms are defined for internal control purposes.

Principle 4: Senior management should ensure that the internal and external factors that could adversely affect the achievement of the bank's objectives are being identified and evaluated. This assessment should cover all the various risks facing the bank (for example, credit risk, country and transfer risk, market risk, interest rate risk, liquidity risk, operational risk, legal risk and reputational risk).

21. Effective risk assessment identifies and considers internal factors (such as the nature of the bank’s activities, the quality of personnel, organisational changes and employee turnover) as well as 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. This risk assessment should be conducted at the level of individual businesses and across the wide spectrum of activities and subsidiaries of the consolidated banking organisation. This can be accomplished through various methods. Effective risk assessment addresses both measurable risks (such as credit, market and liquidity risk) and non-measurable risks (such as operational, legal and reputational risk).

22. The risk assessment process also includes evaluating the risks to determine which are controllable by the bank and which are not. For those risks that are controllable, the bank must assess whether to accept those risks or whether to mitigate the risk through control procedures. 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 concerned.

Principle 5: Senior management should ensure that the risks affecting the achievement of the bank's strategies and objectives are continually being evaluated. Internal controls may need to be revised to appropriately address any new or previously uncontrolled risks.

23. In order for risk assessment, and therefore the system of internal control, to remain effective, senior management needs to continually evaluate the risks affecting the achievement of its goals and react to changing circumstances and conditions. Internal controls may need to be revised to appropriately address any new or previously uncontrolled risks. For example, as financial innovation occurs, a bank needs to evaluate new financial instruments and market transactions and consider the risks associated with these activities. Often these risks can be best understood when considering how various scenarios (economic and otherwise) affect the cash flows and earnings of financial instruments and transactions. Thoughtful consideration of the full range of possible problems, from customer misunderstanding to operational failure, will point to important control considerations.

C. Control Activities

Principle 6: Control activities should be an integral part of the daily operations of a bank. Senior management must set up an appropriate control structure to ensure effective internal controls, defining the control activities at every business level. These should include: top level reviews; appropriate activity controls for different departments or divisions; physical controls; periodic checking for compliance with exposure limits; a system of approvals and authorisations; and, a system of verification and reconciliation. Senior management must periodically ensure that all areas of the bank are in compliance with established policies and procedures.

24. Control activities are designed and implemented to address the risks that the bank identified through the risk assessment process described above. Control activities involve three steps: (1) the establishment of policies; (2) the performance of procedures in accordance with those policies; and, (3) verification that the policies are being complied with. Control activities involve all levels of personnel in the bank, including senior management as well as front line personnel. Examples of control activities include:

- *Top level reviews* - Boards of directors and senior management often request presentations and performance reports that enable them to review the bank’s progress toward its goals. For example, senior management may review reports showing actual financial results to date versus the budget. Questions that senior management generates as a result of this review and the ensuing responses prepared by lower levels of management represent a control activity which may

detect problems such as control weaknesses, errors in financial reporting or fraudulent activities.

- *Activity controls* - Department or division level management receives and reviews standard performance and exception reports on a daily, weekly or monthly basis. Functional reviews occur more frequently than top level reviews and usually are more detailed. For instance, a manager of commercial lending may review weekly reports on delinquencies, payments received, and interest income earned on the portfolio, while the senior credit officer may review similar reports on a monthly basis and in a more summarised form that includes all lending areas. Like the top level review, the questions that are generated as a result of reviewing the reports and the responses to those questions represent the control activity.
- *Physical controls* - Physical controls generally focus on restricting access to physical assets, including securities and other financial assets. Control activities include physical limitations, dual custody, and periodic inventories.
- *Compliance with exposure limits* - The establishment of prudent limits on risk exposures is an important aspect of risk management. For example, compliance with limits for borrowers and other counterparties reduces the bank's concentration of credit risk and helps to diversify its risk profile. Consequently, an important aspect of internal controls is the periodic review of compliance with such limits.
- *Approvals and authorisations* - Requiring approval and authorisation for transactions over certain limits ensures that an appropriate level of management is aware of the transaction or situation, and helps to establish accountability.
- *Verifications and reconciliations* - Verifications of transaction details and activities and the output of risk management models used by the bank are important control activities. Periodic reconciliations, such as those comparing cash flows to account records and statements, may identify activities and records that need correction. Consequently, the results of these verifications should be periodically reported to the appropriate levels of management.

25. Control activities are most effective when they are viewed by management and all other personnel as an integral part of, rather than an addition to, the daily operations of the bank. When controls are viewed as an addition to the day-to-day operations, they are often seen as less important and may not be performed in situations where individuals feel pressured to complete activities in a limited amount of time. In addition, controls that are an integral part of the daily operations enable quick responses to changing conditions and avoid unnecessary costs. As part of fostering the appropriate control culture within the bank, senior

management should ensure that adequate control activities are an integral part of the daily functions of all relevant personnel.

26. It is not sufficient for senior management to simply establish appropriate policies and procedures for the various activities and divisions of the bank. They must periodically ensure that all areas of the bank are in compliance with such policies and procedures and also determine that existing policies and procedures remain adequate. This function is usually carried out as part of the internal audit department.

Principle 7: Senior management should ensure that there is appropriate segregation of duties and that personnel are not assigned conflicting responsibilities. Areas of potential conflicts of interest should be identified, minimised, and carefully monitored.

27. In reviewing major banking losses caused by poor internal controls, supervisors typically find that one of the major causes of such losses is the lack of adequate segregation of duties. Assigning conflicting duties to one individual (for example, responsibility for both the front and back offices of a trading function) gives that person access to assets of value and the ability to manipulate financial data for personal gain or to conceal losses. Consequently, certain duties within a bank should be split among various individuals in order to reduce the risk of manipulation of financial data or misappropriation of assets.

28. Segregation of duties is not limited to situations involving simultaneous front and back office control by one individual. It can also result in serious problems when there are not appropriate controls in those instances where an individual has responsibility for:

- approval of the disbursement of funds and the actual disbursement;
- customer and proprietary accounts;
- transactions in both the "banking" and "trading" books;
- informally providing information to customers about their positions while marketing to the same customers;
- assessing the adequacy of loan documentation and monitoring the borrower after loan origination; and,
- any other areas where significant conflicts of interest emerge and are not mitigated by other factors.

29. Areas of potential conflict should be identified, minimised, and carefully monitored. There should also be periodic reviews of the responsibilities and functions of key individuals to ensure that they are not in a position to conceal inappropriate actions.

D. Information and Communication

Principle 8: Senior management should ensure that there are adequate and comprehensive internal financial, operational and compliance data, as well as external

market information about events and conditions that are relevant to decision making. Information should be reliable, timely, accessible, and provided in a consistent format.

30. Adequate information and effective communication are essential to the proper functioning of a system of internal control. From the bank's perspective, in order for information to be useful, it must be relevant, reliable, timely, accessible, and provided in a consistent format. Information includes internal financial, operational and compliance data, as well as external market information about events and conditions that are relevant to decision making. Internal information is part of a record-keeping process that should include established procedures for record retention.

Principle 9: Senior management should establish effective channels of communication to ensure that all staff are fully aware of policies and procedures affecting their duties and responsibilities and that other relevant information is reaching the appropriate personnel.

31. Without effective communication, information is useless. Senior management of banks need to establish effective paths of communication in order to ensure that the necessary information is reaching the appropriate people. This information relates both to the operational policies and procedures of the bank as well as information regarding the actual operational performance of the organisation.

32. The organisational structure of the bank should facilitate a complete flow of information - upward, downward and across the organisation. A structure that facilitates this flow ensures that information flows upward so that the board of directors and senior management are aware of the business risks and the operating performance of the bank. Information flowing down through an organisation ensures that the bank's objectives, strategies, and expectations, as well as its established policies and procedures, are communicated to lower level management and operations personnel. This communication is essential to achieve a unified effort by all bank employees to meet the bank's objectives. Finally, communication across the organisation is necessary to ensure that information that one division or department knows can be shared with other affected divisions or departments.

Principle 10: Senior management must ensure that there are appropriate information systems in place that cover all activities of the bank. These systems, including those that hold and use data in an electronic form, must be secure and periodically tested.

33. A critical component of a bank's operations is the establishment and maintenance of management information systems that cover the full range of its activities. This information is usually provided through both electronic and non-electronic means. Banks

must be particularly aware of the organisational and internal control requirements related to processing information in an electronic form.

34. Electronic information systems and the use of information technology have risks that must be effectively controlled by banks in order to avoid disruptions to business and potential losses. Controls over information systems and technology should include both general and application controls. General controls are controls over the computer system (i.e., mainframe and end-user terminals) and ensure its continued, proper operation. For example, general controls include back-up and recovery procedures, software development and acquisition policies, maintenance procedures, and access security controls. Application controls are computerised steps within software applications and other manual procedures that control the processing of transactions. Application controls include, for example, edit checks and computer matching. Without adequate controls over information systems and technology, including systems that are under development, banks could experience the loss of data and programs due to inadequate physical and electronic security arrangements, equipment or systems failures, and inadequate backup and recovery procedures. Management decision-making could be adversely affected by unreliable or misleading information provided by systems that are poorly designed and controlled. Information processing could be curtailed or fail entirely if alternate compatible facilities are not available in the event of prolonged equipment failure. In extreme cases, such problems could cause serious difficulties for banks and even jeopardise their ability to conduct key business activities.

E. Monitoring

Principle 11: Senior management should continually monitor the overall effectiveness of the bank's internal controls in helping to achieve the organisation's objectives. Monitoring of key risks should be part of the daily operations of the bank and should include separate evaluations as required.

35. Banking is a dynamic, rapidly evolving industry. Banks must continually monitor and evaluate their internal control systems in light of changing internal and external conditions, and must enhance these systems as necessary to maintain their effectiveness.

36. Monitoring the effectiveness of internal controls should be part of the daily operations of the bank but also include separate periodic evaluations of the overall internal control process. The frequency of monitoring different activities of a bank should be determined by considering the risks involved and the frequency and nature of changes occurring in the operating environment. Ongoing monitoring activities can offer the advantage of quickly detecting and correcting deficiencies in the system of internal control. Such monitoring is most effective when the system of internal control is integrated into the operating environment and produces regular reports for review. Examples of ongoing

monitoring include the review and approval of journal entries, and management review and approval of exception reports.

37. In contrast, separate evaluations typically detect problems only after the fact; however, separate evaluations allow an organisation to take a fresh, comprehensive look at the effectiveness of the internal control system and specifically at the effectiveness of the monitoring activities. Separate evaluations of the internal control system often take the form of self-assessments when persons responsible for a particular function determine the effectiveness of controls for their activities. The documentation and the results of the evaluations are then reviewed by senior management. All levels of review should be adequately documented and reported on a timely basis to the appropriate level of management.

Principle 12: There should be an effective and comprehensive internal audit of the internal control system carried out by appropriately trained and competent staff. The internal audit function, as part of the monitoring of the system of internal controls, should report directly to the board of directors or its audit committee, and to senior management.

38. The internal audit function is an important part of the ongoing monitoring of the system of internal controls because it provides an independent assessment of the adequacy of, and compliance with, the established controls. By reporting directly to the board of directors or its audit committee, and to senior management, the internal auditors provide unbiased information about line activities. Due to the important nature of this function, internal audit must be staffed with competent, well-trained individuals who have a clear understanding of their role and responsibilities. The frequency and extent of internal audit review and testing of the internal controls within a bank should be consistent with the nature, complexity, and risk of the organisation’s activities. In all cases, it is critical that the internal audit function is independent from the day-to-day functioning of the bank and that it has access to all activities conducted by the banking organisation.

39. It is important that the internal audit function reports directly to the highest levels of the banking organisation, typically the board of directors or its audit committee, and to senior management. This allows for the proper functioning of corporate governance by giving the board information that is unaltered in any way by the levels of management that the reports cover. The board should also reinforce the independence of the internal auditors by having such matters as their compensation or budgeted resources determined by the board or the highest levels of management rather than by managers who are affected by the work of the internal auditors.

Principle 13: Identified internal control deficiencies should be reported in a timely manner to the appropriate management level and addressed promptly. Material internal control deficiencies should be reported to senior management and the board of directors.

40. Internal control deficiencies, or ineffective policies or procedures, should be reported to the appropriate person(s) as soon as they are identified, with serious matters reported to senior management and the board of directors. Once deficiencies or ineffective policies or procedures are reported, it is important that management corrects the deficiencies on a timely basis. The internal auditors should conduct follow-up reviews and immediately inform senior management or the board of any uncorrected deficiencies. In order to ensure that all deficiencies are addressed in a timely manner, management should establish a system to track internal control weaknesses and actions taken to rectify them.

IV. Evaluation of Internal Control Systems By Supervisory Authorities

Principle 14: Supervisors should require that all banks, regardless of size, have an effective system of internal controls that is consistent with the nature, complexity, and risk of their on- and off-balance-sheet activities and that responds to changes in the bank's environment and conditions. In those instances where supervisors determine that a bank's internal control system is not adequate (for example, does not cover all of the principles contained in this document), they should take action against the bank to ensure that the internal control system is improved immediately.

41. Although the board of directors and senior management bear the ultimate responsibility for an effective system of internal controls, supervisors should assess the internal control system in place at individual banks as part of their ongoing supervisory activities. The supervisors should also determine whether individual bank management gives prompt attention to any problems that are detected through the internal control process.

42. Supervisors should require the banks they supervise to have strong control cultures and should take a risk-focused approach in their supervisory activities. This includes a review of the adequacy of internal controls. It is important that supervisors not only assess the effectiveness of the overall system of internal controls, but also evaluate the controls over high risk areas (e.g., areas with characteristics such as unusual profitability, rapid growth, or new business activity). Bank supervisors should place special emphasis on written policies and procedures as a key communication mechanism.

43. Supervisors, in evaluating the internal control systems of banks, may choose to direct special attention to activities or situations that historically have been associated with internal control breakdowns leading to substantial losses. Certain changes in a bank's environment should be the subject of special consideration to see whether accompanying revisions are needed in the internal control system. These changes include: (1) a changed operating environment; (2) new personnel; (3) new or revamped information systems; (4) areas/activities experiencing rapid growth; (5) new technology; (6) new lines, products, activities (particularly complex ones); (7) corporate restructurings, mergers and acquisitions; and (8) expansion or acquisition of foreign operations (including the impact of changes in the related economic and regulatory environments).

44. To evaluate the quality of internal controls, supervisors can take a number of approaches. Supervisors can evaluate the work of the internal audit department of the bank through review of its work papers, including the risk assessment methodology used. If satisfied with the quality of the internal audit department's work, supervisors can use the reports of internal auditors as a primary mechanism for identifying control problems in the bank, or for identifying areas of potential risk that the auditors have not recently reviewed. Some supervisors may use a self-assessment process, in which management reviews the

internal controls on a business-by-business basis and certifies to the supervisor that its controls are adequate for its business. Other supervisors may require periodic external audits of key areas, where the supervisor defines the scope. And finally, supervisors may combine one or more of the above techniques with their own on-site reviews or examinations of internal controls.

45. Supervisors in many countries conduct on-site examinations and a review of internal controls is an integral part of such examinations. An on-site review could include both a review of the business process and a reasonable level of transaction testing in order to obtain an independent verification of the bank's own internal control processes.

46. An appropriate level of transaction testing should be performed to verify:

- the adequacy of, and adherence to, internal policies, procedures and limits;
- the accuracy and completeness of management reports and financial records; and
- the reliability (i.e., whether it functions as management intends) of specific controls identified as key to the internal control element being assessed.

47. In order to evaluate the effectiveness of the five internal control elements of a banking organisation (or a unit/activity thereof) supervisors should:

- identify the internal control objectives that are relevant to the organisation, unit or activity under review (e.g., lending, investing, accounting);
- evaluate the effectiveness of the internal control elements, not just by reviewing policies and procedures, but also by reviewing documentation, discussing operations with various levels of bank personnel, observing the operating environment, and testing transactions;
- share supervisory concerns about internal controls and recommendations for their improvement with the board of directors and management on a timely basis, and;
- determine that, where deficiencies are noted, corrective action is taken in a timely manner.

48. Banking supervisory authorities that do not conduct routine on-site examinations typically make use of the work of external auditors. In those instances, the external auditors should be performing the review of the business process and the transaction testing described above.

49. In all instances, bank supervisors should review the external auditors' observations and recommendations regarding the effectiveness of internal controls and determine that bank management and the board of directors have addressed the concerns and recommendations expressed by the external auditors. The level and nature of control problems found by

auditors should be factored into supervisors’ evaluation of the effectiveness of a bank's internal controls.

50. Supervisors should also encourage bank external auditors to plan and conduct their audits in ways that appropriately consider the possibility of misstatement of banks' financial statements due to fraud. Any fraud found by external auditors, regardless of materiality, should be communicated to the appropriate level of management. Fraud involving senior management and fraud that is material to the entity should be reported to the board of directors and/or audit committee. External auditors may be expected to disclose fraud to certain supervisory authorities or others outside the bank in certain circumstances (subject to national requirements).

51. In reviewing the adequacy of the internal control process at individual banking organisations, supervisors should also determine that the process is effective across business lines and subsidiaries. It is important that supervisors evaluate the internal control process not only at the level of individual businesses or legal entities, but also across the wide spectrum of activities and subsidiaries within the consolidated banking organisation.

V. Roles and Responsibilities of External Auditors

52. Although external auditors are not, by definition, part of a banking organisation and therefore, are not part of its internal control system, they have an important impact on the quality of internal controls through their audit activities, including discussions with management and recommendations for improvement to internal controls. The external auditors provide important feedback on the effectiveness of the internal control system.

53. While the primary purpose of the external audit function is to give an opinion on, or to certify, the annual accounts of a bank, the external auditor must choose whether to rely on the effectiveness of the bank's internal control system. For this reason, the external auditors have to conduct an evaluation of the internal control system in order to assess the extent to which they can rely on the system in determining the nature, timing and scope of their own audit procedures.

54. The exact role of external auditors and the processes they use vary from country to country. Professional auditing standards in many countries require that audits be planned and performed to obtain reasonable assurance that financial statements are free of material misstatement. Auditors also examine, on a test basis, underlying transactions and records supporting financial statement balances and disclosures. An auditor assesses the accounting principles used and significant estimates made by management and evaluates the overall financial statement presentation. In some countries, external auditors are required by the supervisory authorities to provide a specific assessment of the scope, adequacy and effectiveness of a bank's internal control system, including the internal audit system.

55. One consistency among countries, however, is the expectation that external auditors will gain an understanding of a bank's internal control process. The extent of attention given to the internal control system varies by auditor and by bank; however, it is generally expected that the auditor would identify significant weaknesses that exist at a bank and report material weaknesses to management orally or in confidential management letters and, in many countries, to the supervisory authority. Furthermore, external auditors may be subject to special supervisory requirements that specify the way that they evaluate and report on internal controls.

Appendix

Supervisory Lessons Learned from Internal Control Failures

A. Management Oversight and the Control Culture

1. Many internal control failures that resulted in significant losses for banks could have been substantially lessened or even avoided if the board and senior management of the organisations had established strong control cultures. Weak control cultures often had two common elements. First, senior management failed to emphasise the importance of a strong system of internal control through their words and actions, and most importantly, through the criteria used to determine compensation and promotion. Second, senior management failed to ensure that the organisational structure and managerial accountabilities were well-defined. For example, senior management failed to require adequate supervision of key decision-makers and reporting of the nature and conduct of business activities in a timely manner.

2. Senior management may weaken the control culture by promoting and rewarding managers who are successful in generating profits but fail to implement internal control policies or address problems identified by internal audit. Such actions send a message to others in the organisation that internal control is considered secondary to other goals in the organisation, and thus diminish the commitment to and quality of the control culture.

3. Some banks with control problems had organisational structures in which accountabilities were not clearly defined. As a result, a division of the bank was not directly accountable to anyone in senior management. This meant that no senior manager monitored the performance of these activities closely enough to notice unusual activities, financial and otherwise, and no senior manager had a comprehensive understanding of the operations and how profits were being generated. If management had understood the operations of the division, they may have been able to recognise warning signs (such as an unusual relationship of profit to levels of risk), investigate the operations and take steps to reduce the eventual losses. These problems could also have been avoided if line management had reviewed transactions and management information reports and held discussions with appropriate personnel about the nature of business transacted. Such approaches provide line management with an objective look at how decisions are being made and ensures that key personnel are operating within the parameters set by the bank and within the internal control framework.

B. Risk Assessment

4. In the recent past, inadequate risk assessment has contributed to some organisations' internal control problems and related losses. In some cases, the potential high yields associated with certain loans, investments, and derivative instruments distracted

management from the need to thoroughly assess the risks associated with the transactions and devote sufficient resources to the continual monitoring and review of risk exposures. Losses have also been caused when management has failed to update the risk assessment process as the organisation's operating environment changed. For example, as more complex or sophisticated products within a business line are developed, internal controls may not be enhanced to address the more complex products. A second example involves entry into a new business activity without a full, objective assessment of the risks involved. Without this reassessment of risks, the system of internal control may not appropriately address the risks in the new business.

5. As discussed above, banking organisations will set objectives for operational efficiency and effectiveness, reliability in financial reporting and compliance with laws and regulations. Risk assessment entails the identification and evaluation of the risks involved in meeting those objectives. This process helps to ensure that the bank's internal controls are consistent with the nature, complexity and risk of the bank's on- and off-balance sheet activities.

C. Control Activities

6. In reviewing major banking losses caused by poor internal control, supervisors typically find that these banks failed to observe certain key internal control principles. Of these, segregation of duties, one of the pillars of sound internal control systems, was most frequently overlooked by banks that experienced significant losses from internal control problems. Often, senior management assigned a highly regarded individual responsibility for supervising two or more areas with conflicting interests. For example, in several cases, one individual supervised both the front and back offices of a trading desk. This permitted the individual to control transaction initiation (e.g., buying and selling securities or derivatives)as well as the related bookkeeping function. Assigning such conflicting duties to one individual gives that person the ability to manipulate financial data for personal gain or to conceal losses.

7. Segregation of duties is not limited to situations involving simultaneous front and back office control by one individual. It can also result in serious problems when an individual has responsibility for:

- approval of the disbursement of funds and the actual disbursement;
- customer and proprietary accounts;
- transactions in both the "banking" and "trading" books;
- informally providing information to customers about their positions while marketing to the same customers;

- assessing the adequacy of loan documentation and monitoring the borrower after loan origination; and
- any other areas where significant conflicts of interest emerge and are not mitigated by other factors.[4]

8. Shortcomings in control activities, however, reflect the failure of a variety of efforts to determine that business is being conducted in the expected manner, from high-level reviews to maintenance of specific checks and balances in a business process. For example, in several cases management did not appropriately respond to information they were receiving. This information took the form of periodic reports on the results of operations for all divisions of the organisation that informed management of each division's progress in meeting objectives, and allowed them to ask questions if the results were different from their expectations. Often, the divisions that later reported significant losses at first reported profits--far in excess of expectations for the apparent level of risk--that should have concerned senior management. Had thorough top level reviews occurred, senior management may have investigated the anomalous results and found and addressed some of the problems, thus limiting or preventing the losses that occurred. However, because the deviations from their expectations were positive (i.e., profits), questions were not asked and investigations were not started until the problems had grown to unmanageable proportions.

D. Information and Communication

9. Some banks have experienced losses because information in the organisation was not reliable or complete and because communication within the organisation was not effective. Financial information may be misreported internally; incorrect data series from outside sources may be used to value financial positions; and small, but high-risk activities may not be reflected in management reports. In some cases, banks failed to adequately communicate employees' duties and control responsibilities or disseminated policies through channels, such as electronic mail, that did not ensure that the policy was read and retained. As a result, for long periods of time, major management policies were not carried out. In other cases, adequate lines of communication did not exist for the reporting of suspected improprieties by employees. If channels had been established for communication of problems upward through the organisational levels, management would have been able to identify and correct the improprieties much sooner.

---

[4] To illustrate a potential conflict of interest that is mitigated by other controls, an independent loan review, through its monitoring activities of a bank's credit grading system, may compensate for the potential conflict of interest that arises when a person who is responsible for assessing the adequacy of loan documentation also monitors the creditworthiness of the borrower after loan origination.

E. Monitoring

10. Many banks that have experienced losses from internal control problems did not effectively monitor their internal control systems. Often the systems did not have the necessary built-in ongoing monitoring processes and the separate evaluations performed were either not adequate or were not acted upon appropriately by management.

11. In some cases, the absence of monitoring began with a failure to consider and react to day-to-day information provided to line management and other personnel indicating unusual activity, such as exceeded exposure limits, customer accounts in proprietary business activities, or lack of current financial statements from borrowers. In one bank, losses associated with trading activities were being concealed in a fictitious customer account. If the organisation had a procedure in place that required statements of accounts to be mailed to customers on a monthly basis and that customer accounts be periodically confirmed, the concealed losses would likely have been noticed long before they were large enough to cause the failure of the bank.

12. In several other cases, the organisation's division or activity that caused massive losses had numerous characteristics indicating a heightened level of risk such as unusual profitability for the perceived level of risk and rapid growth in a new business activity that was geographically distant from the parent organisation. However, due to inadequate risk assessment, the organisations did not provide sufficient additional resources to control or monitor the high risk activities. In fact in some instances, the high risk activities were operating with less oversight than activities with much lower risk profiles--several warnings from the internal and external auditors regarding the activities of the division were not acted upon by management.

13. While internal audit can be an effective source of separate evaluations, it was not effective in many problem banking organisations. A combination of three factors contributed to these inadequacies: the performance of piecemeal audits, the lack of a thorough understanding of the business processes, and inadequate follow-up when problems were noted. The fragmented audit approach resulted primarily because the internal audit programs were structured as a series of discrete audits of specific activities within the same division or department, within geographic areas, or within legal entities. Because the audit process was fragmented, the business processes were not fully understood by internal audit personnel. An audit approach that would have allowed the auditors to follow processes and functions through from beginning to end (i.e., follow a single transaction through from the point of transaction initiation to financial reporting phase) would have enabled them to gain a better understanding. Moreover, it would have provided the opportunity to verify and test the adequacy of controls at every step of the process.

14. In some cases, inadequate knowledge and training of internal audit staff in trading products and markets, electronic information systems, and other highly sophisticated areas

also contributed to internal audit problems. Because the staff did not have the necessary expertise, they were often hesitant to ask questions when they suspected problems, and when questions were asked, they were more likely to accept an answer than to challenge it.

15. Internal audit may also be rendered ineffective when management does not appropriately follow-up on problems identified by auditors. The delays may have occurred because of a lack of acceptance by management of the role and importance of internal audit. In addition, the effectiveness of internal audit is impaired when senior management and members of the board of directors (or audit committee, as appropriate) failed to receive timely and regular tracking reports that indicate critical issues and the subsequent corrective actions taken by management. This type of periodic tracking device can help senior management confront important issues in a timely manner.