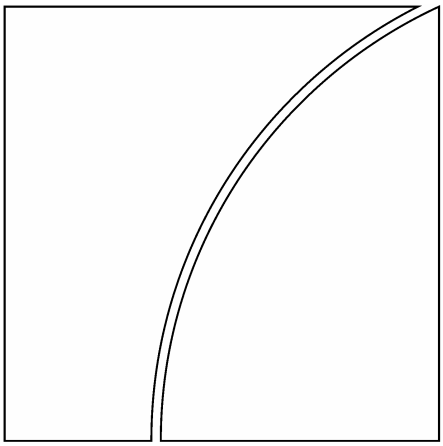
Basel Committee
on Banking Supervision



# Compliance and the compliance function in banks

April 2005

BANK FOR INTERNATIONAL SETTLEMENTS

# Table of contents

## Task Force on Accounting Issues of the Basel Committee on Banking Supervision

Chairman:
Prof Dr Arnold Schilder,
The Netherlands Bank, Amsterdam

| | |
|---|---|
| Banking, Finance and Insurance Commission, Brussels | Mr Marc Pickeur |
| Office of the Superintendent of Financial Institutions Canada, Toronto | Ms Karen Stothers |
| Banking Commission, Paris | Ms Sylvie Matherat |
| Deutsche Bundesbank, Frankfurt am Main | Mr Karl-Heinz Hillen |
| Federal Financial Supervisory Authority (BAFin), Bonn | Mr Ludger Hanenberg |
| Bank of Italy, Rome | Dr Carlo Calandrini |
| Bank of Japan, Tokyo | Mr Keiji Fukuzawa |
| Financial Services Agency, Tokyo | Mr Kenji Oki |
| Surveillance Commission for the Financial Sector, Luxembourg | Mr Guy Haas |
| The Netherlands Bank, Amsterdam | Mr Michael Dobbyn |
| Bank of Spain, Madrid | Mr Anselmo Diaz Fernandez |
| Finansinspektionen, Stockholm | Mr Percy Bargholtz |
| Swiss Federal Banking Commission, Berne | Mr Stephan Rieder |
| Bank of England, London | Mr Ian Michael |
| Financial Services Authority, London | Ms Caroline Morgan |
| Board of Governors of the Federal Reserve System, Washington, DC | Mr Gerald Edwards, Jr |
| Federal Reserve Bank of New York | Mr Arthur Angulo |
| Office of the Comptroller of the Currency, Washington, DC | Mr Zane Blackburn |
| Federal Deposit Insurance Corporation, Washington, DC | Mr Robert Storch |

**Observers**

| | |
|---|---|
| Central Bank of Brazil | Mr Amaro Luiz de Oliveira Gomes |
| European Central Bank | Ms Fatima Pires |
| European Commission, Brussels | Mr Vitorio Pinelli |
| Financial Stability Institute | Mr Jason George |
| Monetary Authority of Singapore, Singapore | Mr Low Kwok Mun |
| Austrian National Bank, Vienna | Mr Martin Hammer |
| Saudi Arabian Monetary Agency, Riyadh | Mr Abdulelah Alobaid |

**Secretariat**

| | |
|---|---|
| Secretariat of the Basel Committee on Banking Supervision, | Ms Donna Bovolaneas |
| Bank for International Settlements | Mr Rory Macfie |

## Introduction

1. As part of its ongoing efforts to address bank supervisory issues and enhance sound practices in banking organisations, the Basel Committee on Banking Supervision (the Committee) is issuing this high level paper on compliance risk and the compliance function in banks. Banking supervisors must be satisfied that effective compliance policies and procedures are followed and that management takes appropriate corrective action when compliance failures are identified.

2. Compliance starts at the top. It will be most effective in a corporate culture that emphasises standards of honesty and integrity and in which the board of directors and senior management lead by example. It concerns everyone within the bank and should be viewed as an integral part of the bank's business activities. A bank should hold itself to high standards when carrying on business, and at all times strive to observe the spirit as well as the letter of the law. Failure to consider the impact of its actions on its shareholders, customers, employees and the markets may result in significant adverse publicity and reputational damage, even if no law has been broken.

3. The expression "*compliance risk*" is defined in this paper as the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct applicable to its banking activities (together, "*compliance laws, rules and standards*").

4. Compliance laws, rules and standards generally cover matters such as observing proper standards of market conduct, managing conflicts of interest, treating customers fairly, and ensuring the suitability of customer advice. They typically include specific areas such as the prevention of money laundering and terrorist financing, and may extend to tax laws that are relevant to the structuring of banking products or customer advice. A bank that knowingly participates in transactions intended to be used by customers to avoid regulatory or financial reporting requirements, evade tax liabilities or facilitate illegal conduct will be exposing itself to significant compliance risk.

5. Compliance laws, rules and standards have various sources, including primary legislation, rules and standards issued by legislators and supervisors, market conventions, codes of practice promoted by industry associations, and internal codes of conduct applicable to the staff members of the bank. For the reasons mentioned above, these are likely to go beyond what is legally binding and embrace broader standards of integrity and ethical conduct.

6. Compliance should be part of the culture of the organisation; it is not just the responsibility of specialist compliance staff. Nevertheless, a bank will be able to manage its compliance risk more effectively if it has a *compliance function* in place that is consistent with the "compliance function principles" discussed below. The expression "*compliance function*" is used in this paper to describe staff carrying out compliance responsibilities; it is not intended to prescribe a particular organisational structure.

7. There are significant differences between banks regarding the organisation of the compliance function. In larger banks, compliance staff may be located within operating business lines, and internationally active banks may also have group and local compliance officers. In smaller banks, compliance function staff may be located in one unit. Separate units have been established in some banks for specialist areas such as data protection and the prevention of money laundering and terrorist financing.

8. A bank should organise its compliance function and set priorities for the management of its compliance risk in a way that is consistent with its own risk management strategy and structures. For instance, some banks may wish to organise their compliance function within their operational risk function, as there is a close relationship between compliance risk and certain aspects of operational risk. Others may prefer to have separate compliance and operational risk functions, but establish mechanisms requiring close co-operation between the two functions on compliance matters.

9. Regardless of how the compliance function is organised within a bank, it should be independent and sufficiently resourced, its responsibilities should be clearly specified, and its activities should be subject to periodic and independent review by the internal audit function. Principles 5 to 8 below describe these high-level principles in more detail, and the supporting guidance sets out sound practices related to the principles. The principles should be applicable to all banks, although it is for individual banks to determine how best they should be implemented. A bank may be able to follow practices other than those set out in this paper which are also sound and which, taken together, demonstrate that its compliance function is effective. The way in which the principles are implemented will depend on factors such as the bank's size, the nature, complexity and geographical extent of its business, and the legal and regulatory framework within which it operates. In smaller banks, for example, it may not be practicable to implement in full some of the specific measures recommended in this paper, yet the bank may be able to take other measures that achieve the same result.

10. The principles in this paper assume a governance structure composed of a board of directors and senior management. The legislative and regulatory frameworks differ across countries and types of entities as regards the functions of the board of directors and senior management. Therefore, the principles set out in this paper should be applied in accordance with the corporate governance structure of each country and type of entity.[1]

11. The expression "bank" is used in this paper to refer generally to banks, banking groups, and to holding companies whose subsidiaries are predominantly banks.

12. This paper should be read in conjunction with a number of related Committee papers, including the following:

- Framework for Internal Control Systems in Banking Organisations (September 1998);
- Enhancing Corporate Governance for Banking Organisations (September 1999);
- Internal Audit in Banks and the Supervisor's Relationship with Auditors (August 2001);
- Customer Due Diligence for Banks (October 2001);
- Sound Practices for the Management and Supervision of Operational Risk (February 2003);

[1] 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.

- International Convergence of Capital Measurement and Capital Standards – A Revised Framework – June 2004; and
- Consolidated KYC Risk Management (October 2004).

13. This paper considers the specific responsibilities of the bank's board of directors and senior management for compliance, before describing the principles that should underpin the bank's compliance function.

## Responsibilities of the board of directors for compliance

***Principle 1***

**The bank's board of directors is responsible for overseeing the management of the bank's compliance risk. The board should approve the bank's compliance policy, including a formal document establishing a permanent and effective compliance function. At least once a year, the board or a committee of the board should assess the extent to which the bank is managing its compliance risk effectively.**

14. As noted in the introduction, a bank's compliance policy will not be effective unless the board of directors promotes the values of honesty and integrity throughout the organisation. Compliance with applicable laws, rules and standards should be viewed as an essential means to this end. As is the case with other categories of risk, the board is responsible for ensuring that an appropriate policy is in place to manage the bank's compliance risk. The board should oversee the implementation of the policy, including ensuring that compliance issues are resolved effectively and expeditiously by senior management with the assistance of the compliance function. The board may, of course, delegate these tasks to an appropriate board level committee (e.g. its audit committee).

## Responsibilities of senior management for compliance

***Principle 2***

**The bank's senior management is responsible for the effective management of the bank's compliance risk.**

15. The following two principles articulate the most important elements of this general principle.

***Principle 3***

**The bank's senior management is responsible for establishing and communicating a compliance policy, for ensuring that it is observed, and for reporting to the board of directors on the management of the bank's compliance risk.**

16. The bank's senior management is responsible for establishing a written compliance policy that contains the basic principles to be followed by management and staff, and explains the main processes by which compliance risks are to be identified and managed through all levels of the organisation. Clarity and transparency may be promoted by making a distinction between general standards for all staff members and rules that only apply to specific groups of staff.

17. The duty of senior management to ensure that the compliance policy is observed entails responsibility for ensuring that appropriate remedial or disciplinary action is taken if breaches are identified.

18. Senior management should, with the assistance of the compliance function:

- at least once a year, identify and assess the main compliance risk issues facing the bank and the plans to manage them. Such plans should address any shortfalls (policy, procedures, implementation or execution) related to how effectively existing compliance risks have been managed, as well as the need for any additional policies or procedures to deal with new compliance risks identified as a result of the annual compliance risk assessment;[2]
- at least once a year, report to the board of directors or a committee of the board on the bank's management of its compliance risk, in such a manner as to assist board members to make an informed judgment on whether the bank is managing its compliance risk effectively; and
- report promptly to the board of directors or a committee of the board on any material compliance failures (e.g. failures that may attract a significant risk of legal or regulatory sanctions, material financial loss, or loss to reputation).

***Principle 4***

**The bank's senior management is responsible for establishing a permanent and effective compliance function within the bank as part of the bank's compliance policy.**

19. Senior management should take the necessary measures to ensure that the bank can rely on a permanent and effective compliance function that is consistent with the following principles.

## Compliance function principles

***Principle 5: Independence***

**The bank's compliance function should be independent.**

20. The concept of independence involves four related elements, each of which is considered in more detail below. First, the compliance function should have a formal status within the bank. Second, there should be a group compliance officer or head of compliance with overall responsibility for co-ordinating the management of the bank's compliance risk. Third, compliance function staff, and in particular, the head of compliance, should not be placed in a position where there is a possible conflict of interest between their compliance responsibilities and any other responsibilities they may have. Fourth, compliance function staff should have access to the information and personnel necessary to carry out their responsibilities.

21. The concept of independence does not mean that the compliance function cannot work closely with management and staff in the various business units. Indeed, a co-operative

[2] See paragraph 41 below.

working relationship between compliance function and business units should help to identify and manage compliance risks at an early stage. Rather, the various elements described below should be viewed as safeguards to help ensure the effectiveness of the compliance function, notwithstanding the close working relationship between the compliance function and the business units. The way in which the safeguards are implemented will depend to some extent on the specific responsibilities of individual compliance function staff.

*Status*

22. The compliance function should have a formal status within the bank to give it the appropriate standing, authority and independence. This may be set out in the bank's compliance policy or in any other formal document. The document should be communicated to all staff throughout the bank.

23. The following issues with respect to the compliance function should be addressed in the document:

- its role and responsibilities;
- measures to ensure its independence;
- its relationship with other risk management functions within the bank and with the internal audit function;
- in cases where compliance responsibilities are carried out by staff in different departments, how these responsibilities are to be allocated among the departments;
- its right to obtain access to information necessary to carry out its responsibilities, and the corresponding duty of bank staff to co-operate in supplying this information;
- its right to conduct investigations of possible breaches of the compliance policy and to appoint outside experts to perform this task if appropriate;
- its right to be able freely to express and disclose its findings to senior management, and if necessary, the board of directors or a committee of the board;
- its formal reporting obligations to senior management; and
- its right of direct access to the board of directors or a committee of the board.

*Head of Compliance*

24. Each bank should have an executive or senior staff member with overall responsibility for co-ordinating the identification and management of the bank's compliance risk and for supervising the activities of other compliance function staff. This paper uses the title "head of compliance" to describe this position.[3]

25. The nature of the reporting line or other functional relationship between staff exercising compliance responsibilities and the head of compliance will depend on how the bank has chosen to organise its compliance function. Compliance function staff who reside in operating business units or in local subsidiaries may have a reporting line to operating business unit management or local management. This is not objectionable, provided such staff also have a reporting line through to the head of compliance as regards their

[3] In some banks, the head of compliance has the title "compliance officer", while in others the title "compliance officer" denotes a staff member carrying out specific compliance responsibilities.

compliance responsibilities. In cases where compliance function staff reside in independent support units (e.g. legal, financial control, risk management), a separate reporting line from staff in these units to the head of compliance may not be necessary. However, these units should co-operate closely with the head of compliance to ensure that the head of compliance can perform his or her responsibilities effectively.

26. The head of compliance may or may not be a member of senior management. If the head of compliance is a member of senior management, he or she should not have direct business line responsibilities. If the head of compliance is not a member of senior management, he or she should have a direct reporting line to a member of senior management who does not have direct business line responsibilities.

27. The supervisor of the bank and the board of directors should be informed when the head of compliance takes up or leaves that position and, if the head of compliance is leaving the position, the reasons for his or her departure. For internationally active banks with local compliance officers, the host country supervisor should be similarly informed of the arrival or departure of the local head of compliance.

*Conflicts of interest*

28. The independence of the head of compliance and any other staff having compliance responsibilities may be undermined if they are placed in a position where there is a real or potential conflict between their compliance responsibilities and their other responsibilities. It is the preference of the Committee that compliance function staff perform only compliance responsibilities. The Committee recognises, however, that this may not be practicable in smaller banks, smaller business units or in local subsidiaries. In these cases, therefore, compliance function staff may perform non-compliance tasks, provided potential conflicts of interest are avoided.

29. The independence of compliance function staff may also be undermined if their remuneration is related to the financial performance of the business line for which they exercise compliance responsibilities. However, remuneration related to the financial performance of the bank as a whole should generally be acceptable.

*Access to information and personnel*

30. The compliance function should have the right on its own initiative to communicate with any staff member and obtain access to any records or files necessary to enable it to carry out its responsibilities.

31. The compliance function should be able to carry out its responsibilities on its own initiative in all departments of the bank in which compliance risk exists. It should have the right to conduct investigations of possible breaches of the compliance policy and to request assistance from specialists within the bank (e.g. legal or internal audit) or engage outside specialists to perform this task if appropriate.

32. The compliance function should be free to report to senior management on any irregularities or possible breaches disclosed by its investigations, without fear of retaliation or disfavour from management or other staff members. Although its normal reporting line should be to senior management, the compliance function should also have the right of direct access to the board of directors or to a committee of the board, bypassing normal reporting lines, when this appears necessary. Further, it may be useful for the board or a committee of the board to meet with the head of compliance at least annually, as this will help the board or

board committee to assess the extent to which the bank is managing its compliance risk effectively.

### *Principle 6: Resources*

**The bank's compliance function should have the resources to carry out its responsibilities effectively.**

33. The resources to be provided for the compliance function should be both sufficient and appropriate to ensure that compliance risk within the bank is managed effectively. In particular, compliance function staff should have the necessary qualifications, experience and professional and personal qualities to enable them to carry out their specific duties. Compliance function staff should have a sound understanding of compliance laws, rules and standards and their practical impact on the bank's operations. The professional skills of compliance function staff, especially with respect to keeping up-to-date with developments in compliance laws, rules and standards, should be maintained through regular and systematic education and training.

### *Principle 7: Compliance function responsibilities*

**The responsibilities of the bank's compliance function should be to assist senior management in managing effectively the compliance risks faced by the bank. Its specific responsibilities are set out below. If some of these responsibilities are carried out by staff in different departments, the allocation of responsibilities to each department should be clear.**

34. Not all compliance responsibilities are necessarily carried out by a "compliance department" or "compliance unit". Compliance responsibilities may be exercised by staff in different departments. In some banks, for example, legal and compliance may be separate departments; the legal department may be responsible for advising management on the compliance laws, rules and standards and for preparing guidance to staff, while the compliance department may be responsible for monitoring compliance with the policies and procedures and reporting to management. In other banks, parts of the compliance function may be located within the operational risk group or within a more general risk management group. If there is a division of responsibilities between departments, the allocation of responsibilities to each department should be clear. There should also be appropriate mechanisms for co-operation among each department and with the head of compliance (e.g. with respect to the provision and exchange of relevant advice and information). These mechanisms should be sufficient to ensure that the head of compliance can perform his or her responsibilities effectively.

*Advice*

35. The compliance function should advise senior management on compliance laws, rules and standards, including keeping them informed on developments in the area.

*Guidance and education*

36. The compliance function should assist senior management in:

- educating staff on compliance issues, and acting as a contact point within the bank for compliance queries from staff members; and

- establishing written guidance to staff on the appropriate implementation of compliance laws, rules and standards through policies and procedures and other documents such as compliance manuals, internal codes of conduct and practice guidelines.

*Identification, measurement and assessment of compliance risk*

37. The compliance function should, on a pro-active basis, identify, document and assess the compliance risks associated with the bank's business activities, including the development of new products and business practices, the proposed establishment of new types of business or customer relationships, or material changes in the nature of such relationships. If the bank has a new products committee, compliance function staff should be represented on the committee.

38. The compliance function should also consider ways to measure compliance risk (e.g. by using performance indicators) and use such measurements to enhance compliance risk assessment. Technology can be used as a tool in developing performance indicators by aggregating or filtering data that may be indicative of potential compliance problems (e.g. an increasing number of customer complaints, irregular trading or payments activity, etc).

39. The compliance function should assess the appropriateness of the bank's compliance procedures and guidelines, promptly follow up any identified deficiencies, and, where necessary, formulate proposals for amendments.

*Monitoring, testing and reporting*

40. The compliance function should monitor and test compliance by performing sufficient and representative compliance testing. The results of the compliance testing should be reported up through the compliance function reporting line in accordance with the bank's internal risk management procedures.

41. The head of compliance should report on a regular basis to senior management on compliance matters. The reports should refer to the compliance risk assessment that has taken place during the reporting period, including any changes in the compliance risk profile based on relevant measurements such as performance indicators, summarise any identified breaches and/or deficiencies and the corrective measures recommended to address them, and report on corrective measures already taken. The reporting format should be commensurate with the bank's compliance risk profile and activities.

*Statutory responsibilities and liaison*

42. The compliance function may have specific statutory responsibilities (e.g. fulfilling the role of anti-money laundering officer). It may also liaise with relevant external bodies, including regulators, standard setters and external experts.

*Compliance programme*

43. The responsibilities of the compliance function should be carried out under a compliance programme that sets out its planned activities, such as the implementation and review of specific policies and procedures, compliance risk assessment, compliance testing, and educating staff on compliance matters. The compliance programme should be risk-based and subject to oversight by the head of compliance to ensure appropriate coverage across businesses and co-ordination among risk management functions.

### *Principle 8: Relationship with Internal Audit*

**The scope and breadth of the activities of the compliance function should be subject to periodic review by the internal audit function.**

44. Compliance risk should be included in the risk assessment methodology of the internal audit function, and an audit programme that covers the adequacy and effectiveness of the bank's compliance function should be established, including testing of controls commensurate with the perceived level of risk.

45. This principle implies that the compliance function and the audit function should be separate, to ensure that the activities of the compliance function are subject to independent review. It is important, therefore, that there is a clear understanding within the bank as to how risk assessment and testing activities are divided between the two functions, and that this is documented (e.g. in the bank's compliance policy or in a related document such as a protocol). The audit function should, of course, keep the head of compliance informed of any audit findings relating to compliance.

## Other matters

### *Principle 9: Cross-border issues*

**Banks should comply with applicable laws and regulations in all jurisdictions in which they conduct business, and the organisation and structure of the compliance function and its responsibilities should be consistent with local legal and regulatory requirements.**

46. Banks may conduct business internationally through local subsidiaries or branches, or in other jurisdictions where they do not have a physical presence. Legal or regulatory requirements may differ from jurisdiction to jurisdiction, and may also differ depending on the type of business conducted by the bank or the form of its presence in the jurisdiction.

47. Banks that choose to conduct business in a particular jurisdiction should comply with local laws and regulations. For example, banks operating in subsidiary form must satisfy the legal and regulatory requirements of the host jurisdiction. Certain jurisdictions may also have special requirements in the case of foreign bank branches. It is for local businesses to ensure that compliance responsibilities specific to each jurisdiction are carried out by individuals with the appropriate local knowledge and expertise, with oversight from the head of compliance in co-operation with the bank's other risk management functions.

48. The Committee recognises that a bank may choose to carry on business in various jurisdictions for a variety of legitimate reasons. Nevertheless, procedures should be in place to identify and assess the possible increased reputational risk to the bank if it offers products or carries out activities in certain jurisdictions that would not be permitted in its home jurisdiction.

### *Principle 10: Outsourcing*

**Compliance should be regarded as a core risk management activity within the bank. Specific tasks of the compliance function may be outsourced, but they must remain subject to appropriate oversight by the head of compliance.**

49. The Joint Forum (i.e. the Basel Committee on Banking Supervision, the International Organization of Securities Commissions, and the International Association of Insurance Supervisors) has recently developed high-level principles for outsourcing by regulated entities, to which banks are encouraged to refer.[4]

50. A bank should ensure that any outsourcing arrangements do not impede effective supervision by its supervisors. Regardless of the extent to which specific tasks of the compliance function are outsourced, the board of directors and senior management remain responsible for compliance by the bank with all applicable laws, rules and standards.

[4] The Joint Forum – "Outsourcing in Financial Services" – February 2005 (available at www.bis.org).