

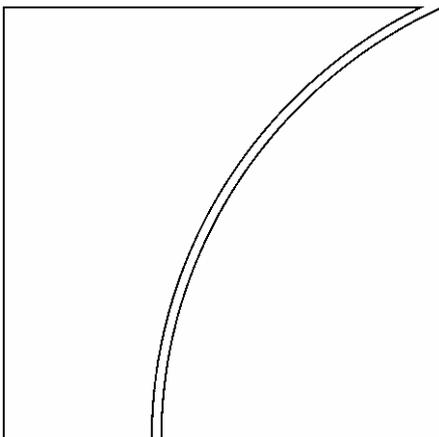
Basel Committee on Banking Supervision

Consultative Document

The compliance function in banks

Issued for comment by 31 January 2004

October 2003



BANK FOR INTERNATIONAL SETTLEMENTS

Table of contents

| | |
|---|---|
| Introduction | 1 |
| Definition of compliance function | 3 |
| Responsibilities of the board of directors for compliance | 3 |
| Principle 1 | 3 |
| Responsibilities of senior management for compliance..... | 3 |
| Principle 2..... | 3 |
| Principle 3..... | 4 |
| Compliance function principles | 4 |
| Status | 4 |
| Principle 4..... | 4 |
| Independence..... | 5 |
| Principle 5..... | 5 |
| Role and responsibilities | 6 |
| Principle 6..... | 6 |
| Compliance function staff | 7 |
| Principle 7..... | 7 |
| Principle 8..... | 7 |
| Cross-border issues | 7 |
| Principle 9..... | 7 |
| The relationship with internal audit..... | 8 |
| Principle 10..... | 8 |
| Outsourcing | 8 |
| Principle 11..... | 8 |

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

Chairman:
Prof Dr Arnold Schilder,
De Nederlandsche Bank, Amsterdam

| | |
|---|--|
| Commission Bancaire et Financière, Brussels | Mr Marc Pickeur |
| Office of the Superintendent of Financial Institutions Canada, Toronto | Ms Donna Bovolaneas |
| Commission Bancaire, Paris | Ms Sylvie Matherat |
| Deutsche Bundesbank, Frankfurt am Main | Mr Karl-Heinz Hillen |
| Bundesaufsichtsamt für das Kreditwesen, Bonn | Mr Ludger Hanenberg |
| Banca d'Italia, Rome | Dr Carlo Calandrini |
| Bank of Japan, Tokyo | Mr Keiji Fukuzawa |
| Financial Services Agency, Tokyo | Mr Kenji Oki |
| Commission de Surveillance du Secteur Financier, Luxembourg | Mr Guy Haas |
| De Nederlandsche Bank, Amsterdam | Mr Michael Dobbyn |
| Banco de España, Madrid | Mr Anselmo Diaz Fernandez |
| Finansinspektionen, Stockholm | Mr Peter Fredby |
| Eidgenössische Bankenkommision, Bern | Mr Stephan Rieder |
| Bank of England, London | Mr Ian Michael |
| Financial Services Authority, London | Mr Tom Barrett |
| Board of Governors of the Federal Reserve System, Washington, DC | Mr Gerald Edwards, Jr |
| Federal Reserve Bank of New York | Ms Zahra El-Mekkawy |
| Office of the Comptroller of the Currency, Washington, DC | Mr Zane Blackburn |
| Federal Deposit Insurance Corporation, Washington, DC | Mr Robert Storch |
| Observers | |
| European Commission, Brussels | Mr Vittorio Pinelli |
| Oesterreichische Nationalbank, Vienna | Mr Martin Hammer |
| Saudi Arabian Monetary Agency, Riyadh | Mr Abdulelah Alobaid |
| Monetary Authority of Singapore, Singapore | Mr Timothy Ng |
| Secretariat | |
| Secretariat of the Basel Committee on Banking Supervision Bank for International Settlements | Mr Bengt A Mettinger Mr Rory Macfie |

Comments on this consultative document are welcome. They should be submitted to the Secretariat of the Basel Committee on Banking Supervision at the Bank for International Settlements, CH-4002 Basel, Switzerland by 31 January 2004. Comments may also be submitted via e-mail: baselcommittee@bis.org¹ or by fax: + 41 61 280 9100. Comments on this paper will not be posted on the BIS website.

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 paper on the compliance function in banking organisations.² The purpose of the compliance function is to assist the bank in managing its compliance risk, which can be defined as the risk of legal or regulatory sanctions, financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with all applicable laws, regulations, codes of conduct and standards of good practice (together, “laws, rules and standards”). Compliance risk is sometimes also referred to as integrity risk, because a bank’s reputation is closely connected with its adherence to principles of integrity and fair dealing. Banking supervisors must be satisfied that effective compliance policies and procedures are followed and that management takes appropriate corrective action when breaches of laws, rules and standards are identified.

2. Compliance with laws, rules and standards helps to maintain the bank’s reputation with, and thus meet the expectations of, its customers, the markets and society as a whole. Although compliance with laws, rules and standards has always been important, compliance risk management has become more formalised within the past few years and has emerged as a distinct risk management discipline.

3. This paper serves as basic guidance for banks and sets out banking supervisors’ views on compliance in banking organisations. The principles in this paper are intended to be of general application, even though they will have to be applied within a specific legal and regulatory framework. There are significant differences between banks regarding the organisation and responsibilities of the compliance function. Some banks have adopted a centralised compliance function (i.e. all compliance staff are located in one compliance department), whilst other banks have chosen a more decentralised compliance function (i.e. compliance staff are located in different business lines). Many banks already have a group compliance officer. In some banks, there may be a separate advisory role for the legal function. There are also differences across jurisdictions. In some jurisdictions the compliance function has specific statutory responsibilities, while in others it does not.

4. The Committee recognises that the exact approach chosen by banks in individual countries will depend on various factors, including their size and sophistication and the nature and geographical extent of their activities. Regardless of how the compliance function is organised within a bank, however, two key principles should be observed: first, the role

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

² In this paper, the expression “function” refers to the staff responsible for carrying out specific activities and responsibilities. The expression is not intended to denote any particular organisational structure.

and responsibilities of the compliance function should be clearly defined; and second, the compliance function should be independent from the business activities of the bank.

5. Compliance risk management is most effective when a bank's culture emphasises high standards of ethical behaviour at all levels of the bank. The board of directors and senior management should promote an organisational culture which establishes through both actions and words the expectation of compliance by all employees (including senior management) with laws, rules and standards when conducting the business of the bank. A compliance function within a bank that is organised along the principles set out in this paper should support management in building a robust compliance culture based on ethical standards of behaviour, and thus contributes to effective corporate governance.

6. 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); and
- Sound Practices for the Management and Supervision of Operational Risk (February 2003).

7. 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.³

8. This paper first proposes a definition of "compliance function". It then considers the responsibilities of the board of directors and senior management for compliance. This is followed by a section headed "Compliance function principles", which discusses the organisation and structure of the compliance function within the bank, its role and responsibilities, and other related issues.

9. The principles in this paper apply to banks, banking groups, and to holding companies whose subsidiaries are predominantly banks.

³ 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.

Definition of compliance function

10. A bank's compliance function can be defined as follows:

“An independent function that identifies, assesses, advises on, monitors and reports on the bank's compliance risk, that is, the risk of legal or regulatory sanctions, financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with all applicable laws, regulations, codes of conduct and standards of good practice (together “laws, rules and standards”)”.

11. The applicable laws, rules and standards are principally those relevant to the business activities of the bank. They include those dealing with the prevention of money laundering and terrorist financing, the conduct of business (including issues such as avoiding or mitigating conflicts of interest), privacy and data protection, and consumer credit (if a bank engages in consumer credit business). They may also extend beyond the business activities of the bank to areas such as employment and tax law, depending on the approach adopted by the supervisory authority or the bank itself.

12. The applicable laws, rules and standards are likely to have various sources, including primary legislation, rules and standards issued by supervisors, market conventions, codes of practice promoted by industry associations, and internal codes of conduct applicable to the staff members of the bank. They are likely to go beyond what is legally binding and embrace broader norms of integrity and fair dealing.

Responsibilities of the board of directors for compliance

Principle 1

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

13. A bank's compliance policy will not be effective unless there is a clear commitment by the board of directors to promoting 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. 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.

Responsibilities of senior management for compliance

Principle 2

The bank's senior management is responsible for establishing a compliance policy, ensuring that it is observed and reporting to the board of directors on its ongoing implementation. Senior management is also responsible for assessing whether the compliance policy is still appropriate.

14. There should be a written compliance policy that identifies the main compliance risk issues facing the bank and explains how the bank intends to manage them. The policy should contain the basic principles to be followed by all staff members (including senior management), as well as a coherent framework for the implementation of more detailed guidance to staff members as circumstances require. 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.

15. 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.

16. Senior management should:

- at least once a year, review the compliance policy and its ongoing implementation to ensure that the policy is still appropriate;
- at least once a year, report to the board of directors or a committee of the board on matters relevant to the compliance policy and its implementation, including recommending any necessary changes to the policy; the reports should assist board members to make an informed judgment as to 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 breaches of laws, rules and standards.

Principle 3

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.

17. Senior management should take the necessary measures to ensure that the bank can rely on a permanent and effective compliance function with sufficient resources.

Compliance function principles

Status

Principle 4

The bank's compliance function should have a formal status within the bank. This is best achieved by a charter or other formal document approved by the board of directors that sets out the function's standing, authority and independence.

18. The following issues should be addressed in the charter or other formal document:

- measures to ensure the independence of the compliance function from the business activities of the bank;
- its role and responsibilities;
- its relationship with other functions or units within the bank;
- its right to obtain access to information necessary to carry out its responsibilities;
- its right to conduct investigations of possible breaches of the compliance policy and to appoint outside legal counsel to perform this task if appropriate;

- its formal reporting obligations to senior management and the board of directors; and
- its right of direct access to the board of directors or a committee of the board.

19. The compliance charter or other formal document should be communicated to all staff throughout the bank.

Independence

Principle 5

The bank's compliance function should be independent from the business activities of the bank.

20. 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 must be free to report to senior management and the board or a committee of the board on any irregularities or possible breaches disclosed by its investigations, without fear of retaliation or disfavour from management or other staff members.

21. 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.

22. Independence also requires that the compliance function be provided with sufficient resources to enable it to carry out its responsibilities effectively. Its budget, and the compensation schemes for compliance function staff, should be consistent with the objectives of the compliance function, and therefore should not be dependent on the financial performance of the various business lines.

23. The compliance function within a bank may be either centralised or decentralised. In either case, there should be a head of compliance who should have day-to-day responsibility for managing the activities of the compliance function and to whom all compliance staff should report.⁴ The independence of compliance staff in a decentralised compliance function may be undermined if they report to management within their business unit rather than to the head of compliance.

24. 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 senior management who do not have direct business line responsibilities, and should also have the right to report directly to the board of directors or a committee of the board, bypassing normal reporting lines, when this appears necessary.

25. In smaller banks, compliance function staff may exercise non-compliance tasks, provided these do not create any conflicts of interest with their compliance responsibilities.

⁴ In some banks, the head of compliance is described as the "compliance officer", while in others the expression "compliance officer" denotes any staff member carrying out compliance responsibilities. To avoid any confusion because of this distinction, this paper uses the expression "head of compliance".

For example, compliance staff should not have any revenue-generating responsibilities, such as trading, marketing or advising clients.

Role and responsibilities

Principle 6

The role of the bank's compliance function should be to identify, assess and monitor the compliance risks faced by the bank, and advise and report to senior management and the board of directors about these risks.

26. The responsibilities of the compliance function should include most if not all of the following. Any responsibilities which are not carried out by the compliance function should be carried out by another independent function.

- on a pro-active basis, identifying and assessing the compliance risks associated with the bank's business activities, including in relation to the development of new products and business practices, the proposed establishment of new business or customer relationships, or material changes in the nature of such relationships;
- advising management on the applicable laws, rules and standards, including keeping up-to-date with developments in the applicable laws, rules and standards and advising management accordingly;
- establishing written guidance to staff on the appropriate implementation of the laws, rules and standards through policies and procedures and other documents such as compliance manuals, internal codes of conduct and practice guidelines;
- assessing the appropriateness of internal procedures and guidelines, promptly following up any identified deficiencies in the policies and procedures and, where necessary, formulating proposals for amendments;
- monitoring compliance with the policy by performing regular and comprehensive compliance risk assessment and testing, and reporting on a regular basis to senior management, and if necessary, the board or a committee of the board, on compliance matters; the reports should refer to the compliance risk assessment and testing which has taken place during the reporting period, any identified breaches and/or deficiencies, and the corrective action taken; the reports should also contain information about compliance training provided to compliance function and other bank staff;
- exercising any specific statutory responsibilities (e.g. fulfilling the role of anti-money laundering officer);
- educating staff with respect to compliance with the applicable laws, rules and standards, and acting as a contact point within the bank for compliance queries from staff members; and
- liaising with relevant external bodies, including regulators, standard setters and external legal counsel.

27. As noted above, not all these responsibilities are necessarily carried out by the compliance function. In some banks, for example, legal and compliance are separate functions; the legal function is responsible for advising management on the applicable laws, rules and standards and for preparing guidance to staff, while the compliance function is responsible for monitoring compliance with the policies and procedures and reporting to management. If there is a division of responsibilities between different functions, the allocation of responsibilities to each function should be clear. If appropriate, there should be

formal mechanisms for co-operation between each function and for the exchange of relevant information. The results of any test which is not carried out by the compliance function (e.g., an internal audit or a management control self assessment) but which identifies a specific compliance failure, would be promptly reported to the head of the compliance

28. The responsibilities of the compliance function should be carried out under a compliance programme which sets out its planned activities, such as the implementation and review of specific policies and procedures, compliance testing, and educating staff on compliance matters.

Compliance function staff

Principle 7

The head of compliance is responsible for the day-to-day management of the activities of the compliance function in accordance with the principles set out in this paper.

29. This principle requires appropriate supervision by the head of compliance of the activities of compliance function staff.

30. The supervisor of the bank should be informed when the head of compliance leaves that position.

Principle 8

Staff exercising compliance responsibilities should have the necessary qualifications, experience and professional and personal qualities to enable them to carry out their duties effectively.

31. Appropriate professional qualities would include a sound understanding of the applicable laws, rules and standards and their practical impact on the bank's operations. The professional skills of compliance staff, especially with respect to keeping up-to-date with developments in the applicable laws, rules and standards, should be maintained through regular and systematic education and training.

32. Appropriate personal qualities (as for most other bank staff) would include integrity, a questioning mind, neutrality and independence of judgment, good communication skills, discretion and tact, as well as the capability to robustly challenge others in the organisation on compliance issues.

Cross-border issues

Principle 9

The compliance function for banks that conduct business in other jurisdictions should be structured to ensure that local compliance issues are satisfactorily addressed within the framework of the compliance policy for the bank as a whole.

33. Banks may conduct business internationally through local branches or subsidiaries, or in other jurisdictions in which they do not have a physical presence. As legal and regulatory requirements may differ from jurisdiction to jurisdiction, compliance issues specific to each jurisdiction should be co-ordinated within the structure of the bank's group-wide compliance policy.

34. The organisation and structure of the compliance function and its responsibilities should be consistent with local legal and regulatory requirements.

The relationship with internal audit

Principle 10

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

35. Compliance risk should be included in the risk assessment methodology of the internal audit function, and an audit programme should be established commensurate with the level of risk. The review of compliance activities by the internal audit function should test the controls in place within the bank to ensure compliance with the applicable laws, rules and standards.

36. 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.

Outsourcing

Principle 11

Specific tasks of the compliance function may be outsourced, subject to appropriate oversight by the head of compliance, who should remain an employee of the bank.

37. Compliance risk management should be regarded as a core risk management activity within the bank. Specific tasks of the compliance function (eg compliance testing and monitoring) may be outsourced, however, provided the outsourcing arrangement is overseen by the head of compliance.

38. Regardless of the extent to which 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.