

CIRCULAR BM - 919

October 17, 2001

To: All Licensed Banks in Oman

Sub: Internal Audit Function in Banks

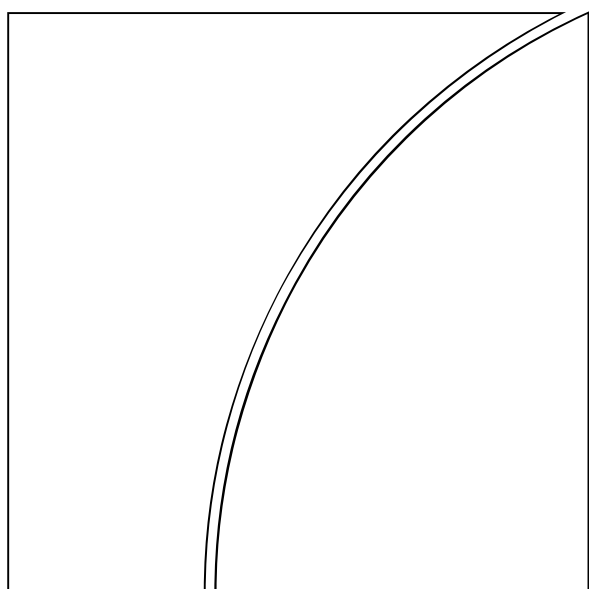
1. As banks are already aware, the Basel Committee on Banking Supervision has recently issued a paper on **Internal Audit in Banks and the Supervisor's Relationship with Auditors**, with the objective of enhancing the internal audit function and harmonising and improving internal audit standards internationally. The paper contains **20 Principles**, which are intended for general application, even though they could be applied within a specific supervisory framework. The Central Bank of Oman also subscribes to the view that strong internal control including audit function is an essential component of sound corporate governance practices in banks.
2. Accordingly, a copy of the paper is enclosed for necessary action. Banks are directed to review their existing internal audit function vis-à-vis the Principles, particularly Principles 1-12, 16, 19 and 20 and chart a definite timeframe for addressing gaps, in the context of the size, complexity of operations, etc. Banks are also directed to carry out a review and prepare an action plan for improving the existing internal audit function, duly approved by the Board of Directors, as soon as possible and in any case not later than December 31, 2001. A copy of the review together with the action plan should be forwarded to the Central Bank of Oman.

3. Banks are required to note that any change in the incumbency of the Head, internal audit and the circumstances for the change should immediately be brought to our notice. The Central Bank of Oman is also interested in one-to-one meeting with the head of the internal audit department when he has been relieved of duties.

Best Regards,

Hamood Sangour Al Zadjali
The Executive President

Basel Committee
on Banking Supervision



**Internal audit in banks and
the supervisor's
relationship with auditors**

August 2001



BANK FOR INTERNATIONAL SETTLEMENTS

Table of Contents

Introduction	1
Definition of internal audit.....	2
Objectives and tasks of the internal audit function.....	2
Principles of internal audit	4
Permanent Function – Continuity	4
Independent function.....	4
Audit charter	5
Impartiality	6
Professional competence.....	6
Scope of activity.....	7
The bank's internal capital assessment procedure.....	8
Functioning of internal audit	9
Working methods and types of audit	9
Risk focus and audit plan	9
Procedures	10
Management of the internal audit department.....	10
The relationship of the supervisory authority with the internal audit department and with the external auditor	11
The relationship of the supervisory authority and the internal audit department	11
The relationship of the internal auditors and the external auditors.....	12
The relationship between the supervisory authority and the external auditor.....	13
Cooperation among the supervisory authority, the external auditors and the internal auditors.....	15
Audit Committee	15
Definition.....	15
Composition, powers and functioning.....	16
Relevant aspects	16
Outsourcing of internal audit	17
Definition.....	17
Outsourcing of the internal audit	17
Outsourcing of internal audit activities in small banks.....	18

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

Chairman:
Prof 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	Mr Philippe Bui
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 Hiroshi Ota
Financial Services Agency, Tokyo	Mr Nobuhiro Hayashi
Commission de Surveillance du Secteur Financier, Luxembourg	Mr Guy Haas
De Nederlandsche Bank, Amsterdam	Mr Michael Dobbyn Mr André van Dorssen
Banco d'España, Madrid	Mr Anselmo Diaz
Finansinspektionen, Stockholm	Mr Hans Hultin
Eidgenössische Bankenkommision, Bern	Mr Stephan Rieder
Bank of England, London	Mr Ian Michael
Financial Services Authority, London	Ms Deborah Chesworth
Board of Governors of the Federal Reserve System, Washington, DC	Mr Gerald Edwards
Federal Reserve Bank of New York	Mr James Beit
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 Tariq Javed
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
--	----------------------

Introduction

1. As part of its ongoing efforts to address bank supervisory issues and enhance supervision through guidance that encourages sound practices, the Basel Committee on Banking Supervision (The Committee) is issuing this paper on internal audit in banking organisations and the relationship of the supervisory authorities with internal and external auditors. Adequate internal controls within banking organisations must be supplemented by an effective internal audit function that independently evaluates the control systems within the organisation. External auditors, on the other hand, can provide an important feedback on the effectiveness of this process. Banking supervisors must be satisfied that effective policies and practices are followed and that management takes appropriate corrective action in response to internal control weaknesses identified by internal and external auditors. Finally, co-operation between the supervisor, the internal auditor and the external auditor optimises supervision.

2. The principles set out in this paper are intended to be of general application, even though they will have to be applied within a specific supervisory framework. There are significant differences across countries as regards the use of on-site and off-site supervisory techniques. Also the degree to which external auditors are used in the supervisory function varies widely. While the exact approach chosen by supervisors in individual countries will depend on these types of factors, all members of the Committee agree on the principles set out in this paper.

3. 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. The principles set out in this paper should be applied in accordance with the national corporate governance structure of each country. It might also be useful to consult the Committee's paper "*Enhancing Corporate Governance for Banking Organisations*" published in September 1999.

4. This document serves as basic guidance for supervisors and it sets out banking supervisors' views on internal audit in banking organisations and the relationship of the supervisory authorities with internal and external auditors. The Committee supports efforts to harmonise and improve internal audit standards internationally. The Committee promotes due consideration of prudential issues in the development of domestic and international internal audit standards.

5. An internal audit function within a bank that is organised along the principles set forth in this paper facilitates the work of bank supervisors. Strong internal control, including an internal audit function, and an independent external audit are part of sound corporate governance which in turn can contribute to an efficient and collaborative working relationship between bank management and bank supervisors. An effective internal audit function is a valuable source of information for bank management, as well as bank supervisors, about the quality of the internal control system.

6. The principles set forth in this paper apply to banks, including those within a banking group, and to holding companies whose subsidiaries are predominantly banks.

7. This document elaborates on the policy guidance issued by the Committee in 1998 entitled "*Framework for Internal Control Systems of Banking Organisations*", particularly the principles about the internal audit function. This 1998 framework provides significant international supervisory guidance on the evaluation of bank internal controls based on an advanced, modern internal control framework.

Definition of internal audit

8. In June 1999, the Board of Directors of the Institute of Internal Auditors approved the following definition of internal audit:

“Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation’s operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.”

9. The need for objectivity and impartiality, especially important for the internal audit department within the banking industry, does not necessarily exclude the possibility that the internal audit department is involved in advising or consulting. Advising senior management on the development of internal controls is often a cost-effective way of ensuring that management makes an informed decision when controls need to be introduced. However, other forms of advising or consulting should be ancillary to the basic function of internal audit, which is an independent appraisal function established within the bank to examine and evaluate its internal control systems, including controls over financial reporting. Internal auditors should not be precluded from analysing and criticising the internal controls that have been put in place by, or at the direction of, senior management even though the auditor provided advice to senior management about internal controls that should be instituted.

10. Some banks have chosen to introduce control self-assessments. These can be described as a formal and documented process whereby management and/or a staff team analyse their activity or function and evaluate the efficiency and effectiveness of the related internal control procedures. These self-assessments may be a useful technique for evaluating the efficiency and effectiveness of internal control without being a substitute for internal audit.

Objectives and tasks of the internal audit function

Principle 1

The bank’s board of directors has the ultimate responsibility for ensuring that senior management establishes and maintains an adequate and effective system of internal controls, a measurement system for assessing the various risks of the bank’s activities, a system for relating risks to the bank’s capital level, and appropriate methods for monitoring compliance with laws, regulations, and supervisory and internal policies. At least once a year, the board of directors should review the internal control system and the capital assessment procedure.

11. The board of directors should regularly verify whether the bank has established an adequate system of internal controls to ensure a well-ordered and prudent conduct of business (with reference to clearly defined objectives). The board should also regularly verify

whether the bank has developed a system for relating risks to the bank's capital level. Finally, the board should ensure that the bank has processes for identifying and adequately controlling the risks incurred in pursuing its business objectives; for testing the integrity, reliability and timeliness of financial information and management information; and for monitoring compliance with laws and regulations, supervisory policies, and internal plans, policies, and procedures.

Principle 2

The bank's senior management is responsible for developing processes that identify, measure, monitor and control risks incurred by the bank. At least once a year, senior management should report to the board of directors on the scope and performance of the internal control system and of the capital assessment procedure.

12. Senior management should maintain an organisational structure that clearly assigns responsibility, authority and reporting relationships and ensures that delegated responsibilities are effectively carried out. Senior management is also responsible for developing risk management processes that identify, measure, monitor and control risks. Finally, senior management sets appropriate internal control policies and monitors the adequacy and effectiveness of the internal control system.

Principle 3

Internal audit is part of the ongoing monitoring of the bank's system of internal controls and of its internal capital assessment procedure, because internal audit provides an independent assessment of the adequacy of, and compliance with, the bank's established policies and procedures. As such, the internal audit function assists senior management and the board of directors in the efficient and effective discharge of their responsibilities as described above.

13. From a general point of view, the scope of internal audit includes:

- the examination and evaluation of the adequacy and effectiveness of the internal control systems;
- the review of the application and effectiveness of risk management procedures and risk assessment methodologies;
- the review of the management and financial information systems, including the electronic information system and electronic banking services;
- the review of the accuracy and reliability of the accounting records and financial reports;
- the review of the means of safeguarding assets;
- the review of the bank's system of assessing its capital in relation to its estimate of risk;
- the appraisal of the economy and efficiency of the operations;
- the testing of both transactions and the functioning of specific internal control procedures;

- the review of the systems established to ensure compliance with legal and regulatory requirements, codes of conduct and the implementation of policies and procedures;
- the testing of the reliability and timeliness of the regulatory reporting; and
- the carrying-out of special investigations.

14. Senior management should ensure that the internal audit department is kept fully informed of new developments, initiatives, products and operational changes to ensure that all associated risks are identified at an early stage.

Principles of internal audit

Permanent Function – Continuity

Principle 4

Each bank should have a permanent internal audit function. In fulfilling its duties and responsibilities, the senior management should take all necessary measures so that the bank can continuously rely on an adequate internal audit function appropriate to its size and to the nature of its operations. These measures include providing the appropriate resources and staffing to internal audit to achieve its objectives.

15. In larger banks and banks with complex operations, internal audit should normally be conducted by an internal audit department with a full-time staff. In small banks, internal audit activities may be outsourced to an outsourcing vendor. Some countries allow small banks to implement a system of independent reviews of key internal controls as an alternative.

16. The guidance given in this document about the internal audit department applies correspondingly to internal audit activities that have been outsourced.

17. The application of principle 4 in the case of a group is discussed under principle 9.

Independent function

Principle 5

The bank's internal audit function must be independent of the activities audited and must also be independent from the every day internal control process. This means that internal audit is given an appropriate standing within the bank and carries out its assignments with objectivity and impartiality.

18. The internal audit department must be able to exercise its assignment on its own initiative in all departments, establishments and functions of the bank. It must be free to report its findings and appraisals and to disclose them internally. The principle of independence entails that the internal audit department operates under the direct control of either the bank's chief executive officer or the board of directors or its audit committee (if one exists), depending on the corporate governance framework.

19. The head of the internal audit department should have the authority to communicate directly, and on his/her own initiative, to the board, the chairman of the board of directors, the

members of the audit committee (if one exists) or the external auditors where appropriate, according to rules defined by each bank in its audit charter ¹. This reporting may cover, for example, bank management's making decisions which are contrary to legal or regulatory provisions.

20. Independence also requires that the internal auditors should not have a conflict of interest with the bank. The compensation scheme for internal auditors should be consistent with the objectives of the internal audit. The internal audit function should be subject to an independent review. This review can be carried out by an independent party like an external auditor, or it can be done by the audit committee, if one exists.

Audit charter

Principle 6

Each bank should have an internal audit charter that enhances the standing and authority of the internal audit function within the bank.

21. An internal audit charter establishes at least:

- the objectives and scope of the internal audit function;
- the internal audit department's position within the organisation, its powers, responsibilities and relations with other control functions; and
- the accountability of the head of the internal audit department.

22. The charter should be drawn up - and reviewed periodically - by the internal audit department; it should be approved by senior management and subsequently confirmed by the board of directors as part of its supervisory role. The audit committee, if one exists, can provide this confirmation.

23. In the charter, the bank's senior management gives the internal audit department the right of initiative and authorises it to have direct access to and communicate with any member of staff, to examine any activity or entity of the bank, as well as to access any records, files or data of the bank, including management information and the minutes of all consultative and decision-making bodies, whenever relevant to the performance of its assignments.

24. The charter should state the terms and conditions according to which the internal audit department can be called upon to provide consulting or advisory services or to carry out other special tasks.

25. The charter should be communicated throughout the organisation.

¹ In some countries, the law specifically encourages organisations to set up avenues for concerns to be raised, either by outsiders or by people inside the organisation. In these countries, the law protects employees who disclose perceived wrongdoing.

Impartiality

Principle 7

The internal audit function should be objective and impartial, which means it should be in a position to perform its assignments free from bias and interference.

26. Objectivity and impartiality entails that the internal audit department itself seeks to avoid any conflict of interest. To this end, staff assignments within the internal audit department should be rotated periodically whenever practicable. Internally recruited auditors should not audit activities or functions they performed within the last twelve months.

27. Impartiality requires that the internal audit department is not involved in the operations of the bank or in selecting or implementing internal control measures. Otherwise it would have to assume responsibility for these activities, which would impair its judgmental independence.

28. However, the need for impartiality does not exclude the possibility that senior management may request from the internal audit department an opinion on specific matters related to the internal control principles to be complied with. For instance, senior management may for the sake of efficiency request an opinion when considering important reorganisations, the start of important or risky new activities, new establishments which are to carry out risky activities, and the setting up or reorganisation of risk control systems, management information systems or information technology systems. However, the eventual development and introduction of these measures should remain the responsibility of management. Indeed, such a consultative function constitutes an ancillary task which should in no way impede the basic tasks or the responsibility and independence of the internal audit department. Subsequent internal audit reports can contain recommendations relating to deficiencies and weaknesses and suggestions for improving internal controls.

Professional competence

Principle 8

The professional competence of every internal auditor and of the internal audit function as a whole is essential for the proper functioning of the bank's internal audit function.

29. The professional competence of each internal auditor as well as his/her motivation and continuing training are prerequisites for the effectiveness of the internal audit department. Professional competence must be assessed taking into account the nature of the role and the auditor's capacity to collect information, to examine, to evaluate and to communicate. In this respect, account should also be taken of the growing technical complexity of banks' activities and the increasing diversity of tasks that need to be undertaken by the internal audit department as a result of developments in the financial sector.

30. Professional competence, and particularly knowledge and experience, within the internal audit department itself also deserve special attention. The main implication of this is that the department as a whole must be competent enough to examine all areas in which the bank operates.

31. Continuously performing similar tasks or routine jobs may negatively affect an internal auditor's capacity for critical judgement. It is therefore recommended, whenever practicable, to rotate staff within the internal audit department. This rotation must be

accomplished in a manner that does not jeopardise the independence of the internal auditors.

32. Professional competence should be maintained through systematic continuing training of each member of the staff. All staff members of the internal audit department should have sufficient up-to-date knowledge of auditing techniques and banking activities.

Scope of activity

Principle 9

Every activity and every entity of the bank should fall within the scope of the internal audit.

33. None of the bank's activities or entities - including the activities of branches and subsidiaries as well as outsourced activities - may be excluded from the internal audit department's scope of investigation. The internal audit department should have access to any records, files or data of the bank, including management information and the minutes of the consultative and decision-making bodies, whenever it is relevant to the performance of its assignments.

34. From a general point of view, the scope of internal audit should include the examination and evaluation of the appropriateness and effectiveness of the internal control system and of the manner in which assigned responsibilities are fulfilled. In many respects, this represents a risk analysis of the bank's internal control system.

35. In particular, the internal audit department should evaluate:

- the bank's compliance with policies and risk controls (both quantifiable and non-quantifiable);
- the reliability (including integrity, accuracy and comprehensiveness) and timeliness of financial and management information;
- the continuity and reliability of the electronic information systems; and
- the functioning of the staff departments.

36. The internal audit department should give adequate consideration to the legal and regulatory provisions covering the bank's operations, including the policies, principles, rules and guidelines issued by the supervisory authority with regard to the manner in which banks are organised and managed. However, this does not imply that the internal audit department should assume the compliance function.

37. Some banks have established separate departments for controlling or monitoring a specific activity or entity of the bank. Such departments are part of the internal control system and therefore their existence does not relieve the internal audit department from examining those specific activities or entities. However, for the sake of efficiency, the internal audit department may, in carrying out its tasks, use the information reported by the various control departments. Nonetheless, the internal audit department remains responsible for the examination and evaluation of the adequate functioning of the internal control of the bank's activity or relevant entity.

38. If a bank has a significant branch abroad, the internal audit department should consider establishing a local office to ensure efficiency and continuity of its work. Such a

local office should be part of the bank's internal audit department and should be organised in such a way as to comply with the principles set out in this document.

39. As separate legal entities, banking or non-banking subsidiaries are responsible for their own internal control and their own internal audit function in accordance with the provisions of this document. At these subsidiaries, the internal audit function may be performed by the internal audit department of the parent company. When subsidiaries have their own internal audit departments, they should report to the parent company's internal audit department. In this situation, the parent company should take all necessary measures, without prejudice to local legal or regulatory provisions and instructions, to ensure that its own internal audit department has unlimited access to all activities and entities of the subsidiaries and that it carries out on-site audits at sufficient intervals.

40. For branches abroad as well as for subsidiaries, the internal auditing principles should be established centrally by the parent bank without prejudice to local, legal and regulatory provisions and instructions. The parent bank should draw up the auditing instructions for the whole group. The parent bank's internal audit department should participate in recruiting and evaluating local internal auditors.

41. In the case of more complex group structures than what is described above, the internal audit function should be organised in such a way as to comply with the principles set out in this document.

The bank's internal capital assessment procedure

Principle 10

Within the framework of the bank's internal capital assessment process, internal audit should carry out regularly an independent review of the risk management system developed by the bank to relate risk to the bank's capital level and the method established for monitoring compliance with internal capital policies.

42. A bank's risk recognition and capital assessment processes differ from the risk management process, which typically focuses more on the review of business strategies developed to maximise the risk/reward trade-off within the different areas of the bank.

43. The bank should clearly identify the individual or department responsible for reviewing the capital assessment procedure. This might be done by the internal audit department or by another individual or department that is sufficiently independent from the operations of the bank.

44. The supervisor's review and evaluation of a bank's internal capital adequacy assessment and its compliance with regulatory capital ratios can draw upon the review of the work done by internal auditors and external auditors, if their work is adequately performed for this purpose.

Functioning of internal audit

Working methods and types of audit

Principle 11

Internal audit includes drawing up an audit plan, examining and assessing the available information, communicating the results, and following up recommendations and issues.

45. There are different types of internal audit, which may include but are not limited to:
- the financial audit, the aim of which is to assess the reliability of the accounting system and information and of resulting financial reports;
 - the compliance audit, the aim of which is to assess the quality and appropriateness of the systems established to ensure compliance with laws, regulations, policies and procedures;
 - the operational audit, the aim of which is to assess the quality and appropriateness of other systems and procedures, to analyse the organisational structures with a critical mind, and to evaluate the adequacy of the methods and resources, in relation to the assignment; and
 - the management audit, the aim of which is to assess the quality of management's approach to risk and control in the framework of the bank's objectives.

46. The internal audit department examines and evaluates the whole of the bank's activities in all its entities. Therefore, it should not focus on one single type of audit, but should use the most appropriate type, depending on the audit objective to be achieved. Furthermore, the internal audit department should not limit itself in this respect to auditing the bank's various departments. Rather, it should also pay special attention to auditing a banking activity through all engaged entities within the bank.

Risk focus and audit plan

47. The management of the internal audit department prepares a plan for all the assignments to be performed. The audit plan includes the timing and frequency of planned internal audit work. This audit plan is based on a methodical control risk assessment. A control risk assessment documents the internal auditor's understanding of the institution's significant activities and their associated risks. The management of the internal audit department should establish the principles of the risk assessment methodology in writing and regularly update them to reflect changes to the system of internal control or work process, and to incorporate new lines of business. The risk analysis examines all of the bank's activities and entities, and the complete internal control system. On the basis of the results of the risk analysis, an audit plan for several years is established, taking into account the degree of risk inherent in the activities. The plan also takes into account expected developments and innovations, the generally higher degree of risk of new activities, and the intention to audit all significant activities and entities within a reasonable time period (audit cycle principle - for example, three years). All those concerns will determine the extent, nature and frequency of the assignments to be performed.

48. The department's audit plan must be realistic, i.e., it must include a time budget for other assignments and activities such as specific examinations, opinions to be given, and training. The plan includes a statement detailing the necessary resources in terms of

personnel and other resources. As for personnel, not only their number but also the necessary professional competence shall be considered. The audit plan should be regularly reviewed and updated whenever necessary.

49. The audit plan should be established by the internal audit department and approved by the bank's chief executive officer or by the board of directors or its audit committee (if one exists). This approval implies that the bank will make the appropriate resources available to the internal audit department.

Procedures

50. For each audit assignment an audit programme should be prepared. The audit programme describes the objectives as well as an outline of the audit work that is considered necessary to achieve them. It is a relatively flexible tool that will have to be adapted and completed according to the risks identified.

51. All audit procedures forming part of the assignment should be documented in working papers. These must reflect the examinations that have been made and emphasise the evaluations formulated in the report. The working papers must be drawn up according to a well-determined method. Such method must provide sufficient information to verify whether the assignment was duly performed and to enable others to check the manner in which it was performed.

52. A written audit report of each assignment is to be issued as quickly as possible. It is transmitted to the auditee and the auditee's management, and - in principle, in executive summary form - to senior management.

53. The audit report presents the purpose and scope of the audit and includes the internal audit department's findings and recommendations, as well as the auditee's responses. It also discloses the items on which a consensus exists at the end of the assignment. The internal audit department indicates the relative importance of the deficiencies found or the recommendations made.

54. The internal audit department maintains a record of the assignments performed and of the reports issued.

55. Senior management should ensure that the internal audit department's concerns are appropriately addressed. Therefore they should approve a procedure established by the internal audit department to ensure the consideration and, if appropriate, the timely implementation of the internal audit department's recommendations.

56. The internal audit department follows up its recommendations to see whether they are implemented. The status of the recommendations is communicated at least every half-year to senior management, to the board of directors or to the audit committee (if one exists), depending on the corporate governance framework.

Management of the internal audit department

Principle 12

The head of the internal audit department should be responsible for ensuring that the department complies with sound internal auditing principles.

57. The head of the internal audit department should ensure compliance with sound internal auditing standards, such as the Institute of Internal Auditors' *Standards for the Professional Practice of Internal Auditing*. In particular, the head of the internal audit department should ensure the establishment of an audit charter, an audit plan, and written policies and procedures for his/her staff. He/she must continuously ensure the professional competence and training of his/her staff and that the necessary resources are available. He/she should also give particular consideration to his/her staff's motivation and to its quality consciousness.

58. The internal audit department should regularly report to and advise senior management and to the board of directors or audit committee (if one exists) on the performance of the internal control system and on the achievement of the internal audit department's objectives. In particular, it should inform senior management and/or the board or audit committee about the progress of the audit plan. As part of its supervisory tasks the board of directors or audit committee should regularly discuss the organisation and resources (both in terms of personnel and otherwise) of the internal audit department, the audit plan, activity reports, and a summary of internal audit's recommendations and the status of their implementation.

The relationship of the supervisory authority with the internal audit department and with the external auditor

The relationship of the supervisory authority and the internal audit department

Principle 13

Bank supervisors should evaluate the work of the bank's internal audit department and, if satisfied, can rely on it to identify areas of potential risk.

59. Supervisory authorities have issued various regulatory provisions covering banks' internal control systems. Although the extent of this regulation may vary across countries, it generally includes some basic principles aimed at promoting an adequate system of controls as well as a regulation with regard to adequate capital. Most supervisors have also laid down policies, practices and procedures in different areas, like the management of credit risk and other core banking risks (such as foreign exchange risks, interest rate risk, liquidity management, computer and telecommunication systems, and risk management of derivatives).

60. To evaluate the quality of internal controls, supervisors can take a number of approaches. One approach is for supervisors to evaluate the work of the internal audit department of the bank, including its testing of senior management's processes that identify, measure, monitor and control risks. 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.

Principle 14

Supervisory authorities should have periodic consultations with the bank's internal auditors to discuss the risk areas identified and the measures taken. At the same occasion, the extent of the collaboration between the bank's internal audit department and the bank's external auditors may also be discussed.

61. Although the internal audit department's task is wide-ranging, it does not set the bank's policies and, except for policies relating to internal control, generally cannot challenge them or the appropriateness of certain policy decisions. This issue is important from a prudential point of view, as an imprudent policy may operate to the detriment of the protection of depositors and other creditors, the interests of shareholders and the proper operation of the credit system. However, this does not preclude the internal audit department from reacting and notifying the board of directors or its audit committee (if one exists) whenever the bank's management makes decisions which are contrary to legal or regulatory provisions or the institution's written policies and procedures.

62. It is a good practice that whenever the head of the bank's internal audit department ceases to act in this capacity, the banking supervisory authority should be informed by the bank's management in a timely manner of the circumstances of this fact. When the head of the internal audit department has been relieved of his/her duties, the Banking supervisory authority should consider meeting with him/her.

Principle 15

Supervisors are encouraged to arrange regular discussions of policy issues jointly with the heads of internal audit departments of the banks under their supervision.

63. It is a good practice for head of the internal audit departments of banks to join forces to enable sector-based consultations between them and the supervisory authority with regard to topics of mutual interest.

The relationship of the internal auditors and the external auditors

Principle 16

Supervisory authorities should encourage consultation between internal and external auditors in order to make their cooperation as efficient and effective as possible.

64. External auditors have an important impact on the quality of internal controls through their audit activities, including discussions with management and the board of directors or audit committee and recommendations for improvement of internal controls.

65. It is generally accepted that the internal audit may be useful in determining the nature, timing and extent of external audit procedures. However, the external auditor has the sole responsibility for the audit opinion on the financial statements. The external auditor should be advised of and have access to relevant internal auditing reports and be kept informed of any significant matter that comes to the internal auditor's attention which may affect the work of the external auditor. Similarly, the external auditor would normally inform the internal auditor of any significant matters which may affect internal auditing.

66. The head of the internal audit department should ensure that work performed by the internal auditor does not unnecessarily duplicate the work of external auditors. Coordination of audit efforts involves periodic meetings to discuss matters of mutual interest, the exchange of audit reports and management letters and a common understanding of audit techniques, methods and terminology.

The relationship between the supervisory authority and the external auditor

Principle 17

Work performed for a bank's supervisory authority by an external auditor should have a legal or contractual basis. Any task assigned by the supervisory authority to the external auditor should be complementary to his/her regular audit work and should be within his/her competence.

67. As explained in International Auditing Practice Statement 1004 "*The relationship between banking supervisors and banks' external auditors*" (which is currently under review), supervisors and external auditors have complementary concerns: the supervisor's notion of stability of the bank is complementary to the auditor's notion of "going concern", and a sound system of internal control as a basis for safe and prudent management is a complement to a system of internal control to establish proper financial statements. In addition, both supervisors and external auditors are concerned with the existence of a proper accounting system.

68. The exact role of external auditors varies from country to country. One constant, however, is the expectation that external auditors will gain an understanding of a bank's internal control system to the extent that it relates to the accuracy of the bank's financial statements. It is also generally expected that material weaknesses identified by the external auditors would be reported to management and, in many countries, to the supervisory authority. Senior management and the board of directors or its audit committee (if one exists) should ensure the implementation of remedial actions related to internal control weaknesses outlined in the reports drawn up by the external auditors. This 'early warning' function of external auditors should be seen in the context of a preventive approach of the supervisors.

69. There are many areas where the work of the supervisor and of the external auditor can be useful to each other. External auditors can obtain helpful insight from information originating from the supervisory authority, for example, through an on-site inspection, management interviews, or other communications with the bank. In countries where external auditors have a close relationship with the supervisory authority, they are often called upon to give an opinion on the functioning and the quality of the internal audit department. Management letters and other reports can provide supervisors with valuable insight into a bank's internal control system.

70. There are also other circumstances in which the external auditor becomes aware of important information which may be relevant to, or may require urgent action on behalf of, the supervisor. Several of those are included in ISA 260 "*Communications of Audit Matters with those Charged with Corporate Governance*"². In addition to the circumstances identified in ISA 260, the following are likely to be relevant to the supervisor

² Ordinarily such matters include:

- The general approach and overall scope of the audit, including any expected limitations thereon, or any additional requirements;
- The selection of, or changes in, significant accounting policies and practices that have, or could have, a material effect on the entity's financial statements;
- The potential effect on the financial statements of any significant risks and exposures, such as pending litigation, that are required to be disclosed in the financial statements;
- Audit adjustments, whether or not recorded by the entity, that have or could have a significant effect on the entity's financial statements;
- Material uncertainties related to events and conditions that may cast significant doubt on the entity's ability to continue as a going concern;

- information that indicates a failure to fulfil one of the requirements for a banking license;
- a serious conflict within the decision-making bodies or the unexpected departure of a manager in a key function;
- information that may indicate a material breach of laws and regulations or the bank's articles of association, charter, or by-laws;
- the intention of the auditor to resign or the removal of the auditor from office; and
- material adverse changes in the risks of the bank's business and possible risks going forward.

71. In many countries, it is expected or required that circumstances of the type indicated above should be timely reported to the supervisory authorities.

72. The relationship between supervisory authorities and external auditors should be based on criteria as explained in International Auditing Practice Statement 1004 (which is currently under review). Particularly important is that there should be a legal basis, or a contractual agreement between the bank and the supervisor, for any work that the external auditor performs for the supervisor. This basis or agreement should address the issue of confidentiality. Equally important is that the external auditor's task for the supervisor must be complementary to his regular audit work and should be within his competence. The supervisory requirements must be clearly defined.

73. In some countries the external auditor's role is extended to perform additional tasks of particular interest for the supervisor like:

- a review of the methods used by the bank to draw up its prudential returns;
- an assessment of the adequacy of the organisation and the internal control system;
- an assessment of the bank's compliance with laws and regulations;
- an evaluation of the bank's internal control systems (including the internal audit department); and
- an expression of an opinion on adherence to appropriate accounting policies.

74. It is recommended that legal measures be taken so that external auditors cannot be held liable for information disclosed in good faith to the supervisory authorities in accordance with applicable laws and regulations.

-
- Disagreements with management about matters that, individually or in aggregate, could be significant to the entity's financial statements or the auditor's report. These communications includes consideration of whether the matter has, or has not, been resolved, and the significance of the matter;
 - Expected modifications to the auditor's report;
 - Other matters warranting attention by those charged with governance, such as material weaknesses in internal control, questions regarding management integrity, and fraud involving management; and Any other matters agreed upon in the terms of the engagement.

75. Supervisory authorities may have information that would be of interest to the external auditor because it might help the external auditor's understanding of the supervisor's concerns or it could significantly affect his/her audit work or other reporting responsibilities. It is important that there exists a legal gateway that enables supervisory authorities to disclose this information to the external auditor when this enables the supervisor to better achieve its objectives.

Cooperation among the supervisory authority, the external auditors and the internal auditors

Principle 18

Cooperation among the supervisor, the external auditor and the internal auditor aims to make the work of all concerned parties more efficient and effective. The cooperation may be based on periodic meetings of the supervisor, the external auditor and internal auditor.

76. The cooperation aims at making the contribution of all concerned parties more efficient and effective, whereby each party concentrates on its own responsibilities.

77. In some countries the cooperation is based on periodic meetings of the supervisory authority, the external auditors and internal auditors. The supervisor may consider the presence of senior management appropriate at these meetings. During these meetings, each party provides information about areas of mutual interest and specific attention is given to the areas that will be examined and the timing of the work. Also, the implementation by the institution of the internal and external auditors' recommendations is discussed by all three parties.

78. Cooperation presupposes a relationship of trust between the bank, its external auditor and the supervisory authority. If there is no trust, co-operation cannot exist. Therefore, supervisory authorities expect to be informed by the bank's senior management about decisions, facts or developments which may have a significant influence on the bank's condition.

Audit Committee

Definition

79. The audit committee is normally regarded as a committee of the board of directors and usually consists of non-executive directors who are independent of management. Its features and denomination may, however, vary across countries.

Principle 19

The creation of a permanent audit committee is a solution to meet the practical difficulties that may arise from the board of directors' task to ensure the existence and maintenance of an adequate system of controls. In addition, such a committee reinforces the internal control system and the internal and external audit. Therefore, banks are encouraged to set up a permanent audit committee, especially if they are involved in complex activities. Banks' subsidiaries should also consider the appropriateness of setting up an audit committee within their board of directors.

Composition, powers and functioning

80. Upon setting up an audit committee, the board of directors should draw up a written charter indicating the audit committee's composition, authority and duties, as well as the way of reporting to the entire board of directors. This document should be approved by the board of directors and reviewed and updated periodically.

81. An audit committee should include at least three members of the board of directors who are not current or former members of senior management. Where members of management are permitted on the audit committee by local law or regulation, they should not constitute a majority of the members of the committee. The members should have a background that is compatible with committee duties. At least one member should have a background in financial reporting, accounting or auditing. For efficiency, the following persons may be allowed to attend regularly the meetings of the audit committee: the chief executive officer or a member of senior management, the head of the internal audit department and the external auditor.

82. The audit committee may request access to any necessary data or records and order any investigation to be performed. The audit committee regularly reports to the board of directors.

Relevant aspects

83. The audit committee should encourage communication between the members of the board of directors, senior management, the internal audit department, the external auditor and the supervisory authority.

84. The audit committee confirms the internal audit charter and the audit plan as well as the resources required (both personnel and tools). It receives the activity reports and the summary of the significant internal auditor's individual recommendations and management's plans for their implementation.

85. The external auditor presents his audit work plan to the audit committee and informs the audit committee of his/her audit conclusions and recommendations.

86. The audit committee regularly discusses:

- the functioning of the internal control system;
- the activities of the internal audit department;
- risk areas of the institution's operations to be covered in the scope of the internal and external audits that year;
- the reliability and accuracy of the financial information provided to management and external users;
- any material accounting or auditing concerns identified as a result of the external or internal audits; and
- the bank's compliance with legal and regulatory provisions, its articles of association, charter, and by-laws, and the rules established by the board of directors.

87. The audit committee should draw up a recommendation to the board of directors for the appointment of the external auditor. The audit committee normally determines and regularly reviews the external auditor's terms of engagement.

88. Some supervisory authorities seek to regularly meet the chairman of each bank's audit committee to enhance their understanding of the corporate governance and system of operation of the bank. These meetings provide an opportunity for the audit committee chairman to discuss any concerns he/she may have about the management of the bank and enable the supervisory authority to form a view on the effectiveness of the audit committee.

Outsourcing of internal audit

Definition

89. An internal audit outsourcing arrangement is a contract between the institution and an outsourcing vendor to provide internal audit services.

90. On the one hand, outsourcing of internal audit activities, especially when it is done on a limited and targeted basis, can bring significant benefits to banks such as access to specialised expertise and knowledge for a special audit project otherwise not available within the organisation. On the other hand, outsourcing may introduce risks to the bank, such as lost or reduced control of the outsourced internal audit activities. Those risks need to be managed and monitored. Furthermore, the outsourcing may affect adversely the supervisory authority's powers to gather information or to require changes in the way that the outsourced activity is carried out. Outsourcing of key banking activities as internal audit may erode the essence of the banking license.

Outsourcing of the internal audit

Principle 20

Regardless of whether internal audit activities are outsourced, the board of directors and senior management remain ultimately responsible for ensuring that the system of internal control and the internal audit, are adequate and operate effectively.

91. Some countries require that a bank's internal audit department should be proficient enough to examine the bank's key activities and to evaluate the functioning, effectiveness and efficiency of internal control over these activities. However, it is accepted that an external expert may carry out certain examinations for which the internal audit department is not - or not sufficiently - proficient. Nevertheless, the factors discussed below concerning the outsourcing of internal audit activities also apply to this case. In addition, the head of the internal audit department should see to it that, whenever practicable, the knowledge input from the expert is integrated into his/her department, possibly by having one or more members of his staff participating in the external expert's work.

92. In other countries banks may use an outsourcing vendor to perform virtually all of the internal audit work. Under such an arrangement, the institution should maintain a senior and experienced individual as head of internal audit and a small internal audit staff. The outsourcing vendor assists staff in determining risks to be reviewed, recommends and performs audit procedures as approved by the head of the internal audit department, and reports its findings jointly with the head of the internal audit department to either the full board or its audit committee. However, it would be unusual in many if not most countries for

a large internationally active bank to outsource all or substantial portions of its internal audit activities.

93. Some countries require the outsourcing vendor to be in all respects completely independent of the external auditor or of the latter's firm and group. Other countries allow outsourcing arrangements to the same external audit firm or group that performs the financial statement audit. However, as this latter arrangement may compromise, in fact or appearance, the independence of an external auditor, banks in these countries should refer to guidance on independence issued by the relevant professional bodies of external accountants or by bank supervisors or other governmental authorities.³

94. The outsourcing vendor must be a competent, financially sound firm with appropriate knowledge and expertise.

95. It is good practice to establish a written contract between the bank and the outsourcing vendor. Senior management should ensure that the bank concludes a contract that can remain valid for a sufficient time period with an outsourcing vendor who has the necessary professional proficiency, taking into account the characteristics of the bank concerned.

96. The contract should define the outsourcing vendor's assignments and responsibilities. The contract should explicitly provide that senior management must give its prior approval to the risk analysis performed by the outsourcing vendor and to the plan that has been established.

97. The contract should also state that senior management or its representative(s), the external auditor(s) or its representative(s), and the supervisory authority have at any time access to the outsourcing vendor's records relating to his assignments, including his/her audit work plan and working papers.

98. The contract should provide that the outsourcing vendor commits him/herself to devote the resources required to effectively perform his assignment under the audit plan. There should be a protocol for changing the terms of the contract, especially for expansion of audit work if significant issues are found.

99. When an institution enters into an outsourcing arrangement, it increases its operating risks. The supervisory authorities expect banks to analyse the impact outsourcing of internal audit activities will have on their overall risk profile and the bank's internal control system. In case the arrangement suddenly terminates, the institution should have a contingency plan. Given that there are a number of possible alternative suppliers in the field of internal audit, the contingency plan will refer most of the time to an alternative vendor. Given the time the new vendor will need, the bank has to consider the need to increase temporarily its own internal audit efforts.

Outsourcing of internal audit activities in small banks

100. It is generally accepted that in certain small banks where the size and the extent of the risks do not justify entrusting the internal audit activities to at least one full-time staff

³ For example the European Commission's Draft Recommendation on Statutory Auditors' Independence and the U.S. Securities and Exchange Commission's Auditor Independence Requirements.

member, all of the internal audit activities can be outsourced to an external vendor. All the principles concerning internal audit remain applicable in the case where all of the internal audit activities are outsourced.

101. In such situations, senior management is responsible for seeing that the recommendations of the audit are addressed and for determining who is responsible for implementing them.