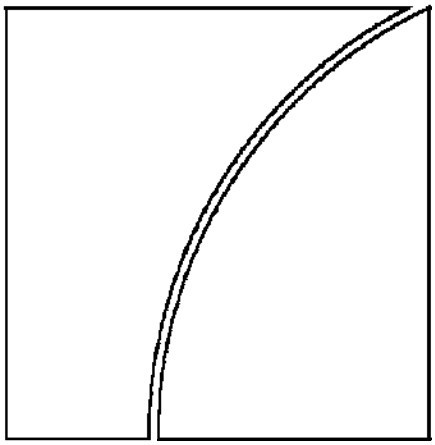
Basel Committee
on Banking Supervision

Consultative document



The internal audit function in banks

December 2011

BANK FOR INTERNATIONAL SETTLEMENTS

This publication is available on the BIS website (www.bis.org).

ISBN 92-9131- 896-5 (print)

ISBN 92-9197- 896-5 (online)

Contents

Members of the Accounting Task Force's Audit Subgroup of the Basel Committee on Banking Supervision

Chairman:
Mr Marc Pickeur
National Bank of Belgium

Representatives in *italics* provided drafting support

Office of the Superintendent of Financial Institutions, Canada	Ms Laural Ross
	Ms Ruby Garg
Bank of France	Ms Nathalie Boutin
Prudential Supervisory Authority, France	Ms Sylvie Marchal
Deutsche Bundesbank, Germany	Ms Dragomira Berberova
Bundesanstalt für Finanzdienstleistungsaufsicht, Germany	Ms Dana Kubis
Banca d'Italia, Italy	Ms Lidja Schiavo
Bank of Japan	Mr Hiroyuki Yoshida
	Ms Keiko Sumida
Financial Services Agency, Japan	Mr Tadashi Tsumori
Commission de Surveillance du Secteur Financier, Luxembourg	Ms Martine Wagner
De Nederlandsche Bank, The Netherlands	Mr Nic van der Ende
Banco d'España, Spain	Ms Barbara Olivares
Financial Services Authority, United Kingdom	Ms Patricia Sucher
	Mr Robert Konowalchuk
Board of Governors of the Federal Reserve System, United States	Mr Terrill Garrison
Office of the Comptroller of the Currency, United States	Mr Robert Riordan
Federal Deposit Insurance Corporation, United States	Mr Harrison Greene
Secretariat	
Secretariat of the Basel Committee on Banking Supervision	Mr Xavier-Yves Zanota

Introduction

1. The Basel Committee on Banking Supervision (the Committee) is issuing this revised supervisory guidance for assessing the effectiveness of the internal audit function in banks, which forms part of the Committee's ongoing efforts to address bank supervisory issues and enhance supervision through guidance that encourages sound practices within banks. The document replaces the 2001 document *Internal audit in banks and the supervisors relationship with auditors*. It takes into account developments in supervisory practices and in banking organisations and incorporates lessons drawn from the recent financial crisis.

2. The Committee's *Principles for Enhancing Corporate Governance*[1] require banks to have an internal audit function with sufficient authority, stature, independence, resources and access to the board of directors. Independent, competent and qualified internal auditors are vital to sound corporate governance.

3. As a strong internal control framework including an independent, effective internal audit function is part of sound corporate governance. Banking supervisors must be satisfied as to the effectiveness of a bank's internal audit function, that effective policies and practices are followed and that management takes appropriate corrective action in response to internal control weaknesses identified by internal auditors. An effective internal audit function provides vital assurance to a bank's board of directors and senior management (and bank supervisors) as to the quality of the bank's internal control system. In doing so, the function helps reduce the risk of loss and reputational damage to the bank.

4. This document addresses supervisory expectations for the internal audit function in banking organisations and the supervisory assessment of that function. This document seeks to promote a strong internal audit function within banking organisations and to provide guidance for the supervisory assessment of this function. It also encourages bank internal auditors to comply with and to contribute to the development of national and international professional standards, such as those issued by The Institute of Internal Auditors, and it promotes due consideration of prudential issues in the development of internal audit standards and practices.

5. This document refers to a management structure comprised of a board of directors and senior management. The Committee recognises that significant differences exist in legislative and regulatory frameworks between countries which shape the role and function of management and governance structures. In some countries the board of directors has the main, if not exclusive, function of overseeing the executive body, often referred to as senior management, and ensuring that it fulfils its responsibilities. For this reason it is sometimes known as a supervisory board that has no executive functions. In contrast, in other countries the board has a broader remit in that it lays down the general framework for the management of the bank. Owing to these differences, the concepts of the board of directors and senior management are used in this document not to identify legal constructs but rather to label two decision-making functions within a bank. The principles set out in this document should be applied in accordance with the applicable national corporate governance structure of each country.

6. For large banks and internationally active banks, an audit committee (or its equivalent) is typically responsible for providing oversight of the bank's internal auditors.

---

[1] BCBS website: http://www.bis.org/publ/bcbs176.pdf

Such a committee is established within the board of directors. Annex 2 of this document provides more details about the responsibilities of audit committees. In this document, references to the board of directors presume appropriate involvement of its audit committee, when one exists. In line with the Committee's *Principles for Enhancing Corporate Governance*, referred to above, this document assumes that large and internationally active banks have an audit committee. Other banks are strongly encouraged to establish such a committee.

7. This guidance applies to all banks, including those within a banking group, and to holding companies whose subsidiaries are predominantly banks. All of these structures are referred to as banks or banking organisations in this document. The extent of application of this guidance should be commensurate with the significance, complexity and international presence of the bank (principle of proportionality).

Overview of the principles

Principles relating to the supervisory expectations relevant to the internal audit function

Principle 1: An effective internal audit function independently and objectively evaluates the quality and effectiveness of a bank's internal control, risk management and governance processes, which assists senior management and the Board of Directors in protecting their organisation and its reputation.

Principle 2: The bank's internal audit function must be independent of the audited activities. This requires that the internal audit function has an appropriate standing within the bank, enabling internal auditors to carry out their assignments with objectivity.

Principle 3: Professional competence, including the knowledge and experience of each internal auditor and of internal auditors collectively, is essential to the effectiveness of the bank's internal audit function.

Principle 4: Internal auditors should act with integrity.

Principle 5: Each bank should have an internal audit charter that articulates the purpose, standing and authority of the internal audit function within the bank.

Principle 6: Every activity (including outsourced activities) and every entity of the bank should fall within the overall scope of the internal audit function.

Principle 7: The internal audit function should ensure adequate coverage of regulatory matters within the audit plan.

Principle 8: Each bank should have a permanent internal audit function.

Principle 9: The bank's board of directors has the ultimate responsibility for ensuring that senior management establishes and maintains an adequate, effective and efficient internal control framework and internal audit function.

Principle 10: The audit committee, or its equivalent, should oversee the bank's internal audit function.

Principle 11: The head of the internal audit department should be responsible for ensuring that the department complies with sound internal auditing standards and with a relevant code of ethics.

Principle 12: The internal audit function should report to the audit committee or the board of directors and should inform senior management about its findings.

Principle 13: Internal audit should both complement and assess operational management, risk management, compliance and other control functions.

Principle 14: The internal audit function in a group structure or holding company structure should be established centrally by the parent bank.

Principle 15: Regardless of whether internal audit activities are outsourced, the board of directors remains ultimately responsible for ensuring that the system of internal control and the internal audit function are adequate and operating effectively.

Principle relating to the relationship of the supervisory authority with the internal audit function

Principle 16: Supervisors should have regular communication with the bank's internal auditors to (i) discuss the risk areas identified by both parties, (ii) understand the risk mitigation measures taken by the bank, and (iii) monitor the bank's response to weaknesses identified.

Principles relating to the supervisory assessment of the internal audit function

Principle 17: Bank supervisors should regularly assess whether the internal audit function has an appropriate standing within the bank and operates according to sound principles.

Principle 18: Supervisors should formally report all weaknesses identified in the internal audit function to the board of directors and require remedial actions.

Principle 19: The supervisory authority should consider the impact of its assessment of the internal audit function on its assessment of the bank's risk profile and on its own supervisory work.

Principle 20: The supervisory authority should be prepared to take informal or formal supervisory actions requiring senior management and the board to remedy any identified deficiencies related to the internal audit function within a specified timeframe and to provide the supervisor with periodic written progress reports.

A. Supervisory expectations relevant to the internal audit function

Principle 1: An effective internal audit function independently and objectively evaluates the quality and effectiveness of a bank's internal control, risk management and governance processes, which assists senior management and the Board of Directors in protecting their organisation and its reputation.

1. The internal audit function

8. The internal audit function plays a crucial role in the ongoing maintenance and assessment of a bank's internal control, risk management and governance – areas in which supervisory authorities have a keen interest. Furthermore, both internal auditors and supervisors use risk based approaches to determine their respective work plans and actions. While internal auditors and supervisors each have a different mandate and are responsible for their own judgments and assessments, they may identify the same or similar/related risks.

9. A widely accepted definition of internal audit published by The Institute of Internal Auditors (The IIA) is:

> "*Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes*."[2]

10. Providing consulting services to senior management on the assessment or development of internal controls is often a cost-effective way of ensuring that management makes informed decisions. This role as a trusted advisor to senior management, while valuable, should be performed in a way that does not compromise the independence and objectivity of the internal audit function. This requires that internal auditors should not assume management responsibility when providing consulting services or design and/or implement internal controls.

2. Key features of the internal audit function

11. The key features described below are essential for the effective operation of an internal audit function.

(a) Independence and objectivity[3]

Principle 2: The bank's internal audit function must be independent of the audited activities. This requires that the internal audit function has an appropriate standing within the bank, enabling internal auditors to carry out their assignments with objectivity.

12. On the basis of the audit plan established by the head of the internal audit function and approved by the board of directors, the internal audit function must be able to perform its assignments on its own initiative in all areas and functions of the bank. It must be free to report its findings and assessments internally through clear reporting lines. The head of internal audit should demonstrate appropriate leadership and have the necessary skills to fulfil his or her responsibility for maintaining the function's independence and objectivity.

---

[2] This definition is part of The Institute of Internal Auditors' *International professional practices framework* (www.theiia.org).

[3] Both 'independence' and 'objectivity' have a specific meaning in an internal audit environment. The Glossary of The Institute of Internal Auditors refers to independence as the freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner. Objectivity is referred to in the Glossary as an unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are made. Objectivity requires that internal auditors do not subordinate their judgement on audit matters to others.

13. The internal audit function should not be involved in designing, selecting, implementing or operating specific internal control measures. However, the independence of the internal audit function should not prevent senior management from requesting input from internal audit on matters related to risk and internal controls. Nevertheless, the development and implementation of internal controls should remain the responsibility of management.

14. Continuously performing similar tasks or routine jobs may negatively affect an individual internal auditor's capacity for critical judgement because of possible loss of objectivity. It is therefore recommended, whenever practicable and without jeopardising competence and expertise, that the internal audit staff rotate periodically within the internal audit function.

15. The independence and objectivity of the internal audit function may be undermined if the staff's remuneration is linked to the financial performance of the business line for which they exercise internal audit responsibilities or to the financial performance of the bank as a whole.

(b) Professional competence and due professional care

Principle 3: Professional competence, including the knowledge and experience of each internal auditor and of internal auditors collectively, is essential to the effectiveness of the bank's internal audit function.

16. Professional competence depends on the auditor's capacity to collect and understand information, to examine and evaluate audit evidence and to communicate with the stakeholders of the internal audit function. This should be combined with suitable methodologies and tools and sufficient knowledge of auditing techniques. Consideration should also be given to ensuring the internal audit staff acquire appropriate ongoing training in order to meet the growing technical complexity of banks' activities and the increasing diversity of tasks that need to be undertaken as a result of the introduction of new products and processes within banks and other developments in the financial sector.

17. Internal auditors collectively should be competent to examine all areas in which the bank operates. When outsourcing arrangements are in place (e.g. when external experts are engaged to support the bank's internal auditors), it is the responsibility of the head of internal audit to maintain adequate oversight and to ensure adequate transfer of knowledge from external experts to the bank's internal audit function.

18. Internal auditors must apply the care and skills expected of a reasonably prudent and competent professional. Due professional care does not imply infallibility; however, internal auditors having limited competence and experience in a particular area should be supervised by more experienced internal auditors.

(c) Professional ethics

Principle 4: Internal auditors should act with integrity.

19. Integrity establishes trust as it requires the internal auditor to be straightforward, honest and truthful. This provides the basis for reliance on the internal auditor's judgement.

20. Internal auditors should respect the confidentiality of information acquired in the course of their duties. They should not use that information for personal gain or malicious action and should be diligent in the protection of information acquired.

21. The head of the internal audit function and all internal auditors should avoid conflicts of interest. Internally recruited internal auditors should not engage in auditing activities for which they have had previous responsibility before a sufficiently long "cooling off" period has elapsed. Moreover, compensation arrangements should not provide incentives for internal auditors to act contrary to the attributes and objectives of the internal audit function.

22. Internal auditors should apply the bank's code of ethics (when there is one) or should adhere to an established international code of ethics for internal auditors, such as that of The Institute of Internal Auditors.[4] A code of ethics should at a minimum address the principles of objectivity, competence, confidentiality and integrity.

3. The internal audit charter

Principle 5: Each bank should have an internal audit charter that articulates the purpose, standing and authority of the internal audit function within the bank.

23. The charter should be drawn up and reviewed periodically by the head of internal audit and approved by the board of directors. It should be available to all internal and external stakeholders of the organisation.

24. At a minimum, an internal audit charter should establish:

- The internal audit function's position within the bank, its authority, its responsibility and its relations with other control functions;
- The purpose and scope of the internal audit function;
- The key features described above under Section A.2, Key features of the internal audit function;
- The obligation of the internal auditors to communicate the results of their engagements and a description of how and to whom this should be done (reporting line);
- The criteria for when and how the internal audit function may outsource some of its engagements to external experts;
- The terms and conditions according to which the internal audit function can be called upon to provide consulting or advisory services or to carry out other special tasks;
- The responsibility and accountability of the head of internal audit;
- A requirement to comply with sound internal auditing standards;
- Procedures for the coordination of the internal audit function with the statutory or external auditor

25. The charter should empower the internal audit function, whenever relevant to the performance of its assignments, to initiate direct communication with any member of staff, to examine any activity or entity, and to access any records, files, data and physical properties of the bank. This includes management information and the minutes of all consultative and decision-making bodies.

---

[4] The Institute of Internal Auditors (The IIA) and the International Ethics Standards Board for Accountants (IESBA) have each issued a code of ethics. Both codes emphasise the importance of the principle of integrity.

4. Scope of activity

Principle 6: Every activity (including outsourced activities) and every entity of the bank should fall within the overall scope of the internal audit function.

26. The scope of internal audit activities should include examination and evaluation of the effectiveness of the internal control framework of the entire bank, including assignment of responsibility and accountability within the bank and appropriate processes to follow up on audit findings and recommendations.

27. The internal audit function should evaluate:

- Effectiveness and efficiency of operations;
- Reliability, effectiveness and integrity of management information systems and processes (including relevance, accuracy and comprehensiveness);
- Monitoring of compliance with laws and regulations, including any requirements from supervisors (see the following sub-section for more details); and
- Safeguarding of assets.

28. The internal audit function should develop an independent and informed view of the risks faced by the bank, based on the information made available to them and their own enquiries and professional competence.

29. The head of internal audit is responsible for establishing an annual internal audit plan that can be part of a multi-year plan. The plan should be based on a risk assessment (including input from senior management and the board) and should be updated at least annually. The head of internal audit should ensure that all entities and all activities of the bank are audited at least once within an appropriate period of time (audit cycle). The board's approval of the audit plan implies that an appropriate budget will be available to support the internal audit function's activities. The budget should be sufficiently flexible to adapt to variations in the internal audit plan in response to changes in the bank's risk profile.

Principle 7: The internal audit function should ensure adequate coverage of regulatory matters within the audit plan.

30. Internal audit should have appropriate capability regarding regulatory matters and undertake regular reviews of such areas. These include policies, processes and governance measures established in response to various regulatory principles, rules and guidance established by the relevant authorities. In particular, the internal audit function of a bank should have the capacity to review key risk management functions, regulatory capital adequacy and liquidity control functions, regulatory reporting functions and regulatory compliance functions.

(a) Risk management

31. A bank's system of risk management supports and reflects its adherence to regulatory provisions and safe and sound banking practices. Therefore, internal audit should include in its scope the following aspects of risk management:

- the organisation and mandates of the risk management functions including market, credit, liquidity, interest rate, operational, and legal risks;
- the adequacy of risk management systems and processes for identifying, measuring, assessing, controlling, responding to, and reporting on all the risks resulting from the bank's activities;

- the integrity of the risk management information systems, including the accuracy, reliability and completeness of the data used; and
- the approval and maintenance of risk models including verification of the consistency, timeliness, independence and reliability of data sources used in such models.

(b) Capital adequacy and liquidity

32. Banks are subject to the global regulatory framework for capital and liquidity as approved by the Committee and implemented in national regulation. This framework contains measures to strengthen regulatory capital and global liquidity. The scope of internal audit should include all provisions of this regulatory framework and in particular the bank's system for identifying and measuring its regulatory capital and assessing the adequacy of its capital resources in relation to the bank's risk exposures and established minimum ratios.

33. Internal audit should review management's process for stress testing its capital levels, taking into account the frequency of such exercises, their purpose (e.g., internal monitoring vs. regulator imposed), the reasonableness of scenarios and the underlying assumptions employed, and the reliability of the processes used.

34. Additionally, the bank's systems and processes for measuring and monitoring its liquidity positions in relation to its risk profile, external environment, and minimum regulatory requirements, should fall within the audit universe.

(c) Regulatory and internal reporting

35. In addition to the matters identified above, internal auditors should regularly evaluate the effectiveness of the process by which the risk and reporting functions interact to produce timely, accurate, reliable and relevant reports for both internal management and the supervisor.

36. This includes standardised reports which record the bank's calculation of its capital resources, requirements and ratios. It may also include public disclosures intended to facilitate transparency and market discipline such as the Pillar 3 disclosures and the reporting of regulatory matters in the bank's public reports.

(d) Compliance[5]

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

38. Compliance laws, rules and standards include 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.

39. The audit of the compliance function should include an assessment of how effectively it fulfils its responsibilities.

---

[5] To be read in conjunction with the Committee's *Compliance and the compliance function in banks,* April 2005.

5. Corporate governance considerations

40. Annex 1 provides an illustrative overview of relevant principles and standards with respect to the internal audit function, corporate governance structure, and communication channels within a generic bank's governance model.

(a) Permanency of the internal audit function

Principle 8: Each bank should have a permanent internal audit function.

41. In fulfilling its duties and responsibilities, senior management and the board should take all the necessary measures to ensure that the bank has a permanent internal audit function commensurate with its size, the nature of its operations and the complexity of its organisation.

42. Internal audit activities should normally be conducted by the bank's own internal audit staff. While internal audit activities may be partially or fully outsourced, the board of directors remains responsible for these activities and for maintaining an internal audit *function* within the bank. Outsourcing of internal audit activities is further addressed in principle 15 and related paragraphs.

(b) Responsibilities of the board of directors and senior management

Principle 9: The bank's board of directors has the ultimate responsibility for ensuring that senior management establishes and maintains an adequate, effective and efficient internal control framework and internal audit function.

43. At least once a year, the board of directors should review the effectiveness and efficiency of the internal control framework based, in part, on information provided by the internal audit function. Moreover, as part of their oversight responsibilities, the board of directors should review the performance of the internal audit function. From time to time, the board of directors should consider commissioning an independent review of the internal audit function.

44. Senior management is responsible for developing an internal control framework that identifies, measures, monitors and controls all risks faced by the bank. It should maintain an organisational structure that clearly assigns responsibility, authority and reporting relationships and ensures that delegated responsibilities are effectively carried out. It is an established practice for senior management to report to the board of directors on the scope and performance of the internal control framework.

45. Senior management should inform the internal audit function of new developments, initiatives, projects, products and operational changes and ensure that all associated risks, known and anticipated, are identified and communicated at an early stage.

46. Senior management should be accountable for ensuring that timely and appropriate actions are taken on all internal audit findings and recommendations.

47. Senior management should ensure that the head of internal audit has available the necessary resources, financial and otherwise, to carry out his or her duties commensurate with the approved annual audit plan.

(c) Responsibilities of the audit committee in relation to the internal audit function

Principle 10: The audit committee, or its equivalent, should oversee the bank's internal audit function

48. This principle applies when the board of directors has established an audit committee. In cases where no audit committee exists, the responsibilities described below should be assumed by the board itself. As explained in paragraph 50 of the Committee's *Principles for Enhancing Corporate Governance,* large banks and internationally active banks should have an audit committee or its equivalent. Other banks are encouraged to establish an audit committee.

49. The audit committee reviews and approves the audit plan and, if any, the audit cycle. It also reviews key audit reports and ensures that senior management is taking necessary and timely corrective actions to address control weaknesses, compliance issues with policies, laws and regulations and other concerns identified and reported by the internal audit function.

50. Annex 2 of this document gives an overview of the responsibilities of an audit committee.

(d) Management of the internal audit department

Principle 11: The head of the internal audit department should be responsible for ensuring that the department complies with sound internal auditing standards and with a relevant code of ethics.

51. The head of the internal audit department should ensure compliance with sound internal auditing standards, such as The Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. In addition, auditors should adhere to a relevant code of ethics (see paragraph 22).

52. The audit committee should ensure that the head of the internal audit function is a person of integrity. This means that he or she will be able to perform his or her work with honesty, diligence, and responsibility. It also implies that these persons always have observed the law and have not been knowingly a party to any illegal activity. The head of internal audit should also ensure that the internal audit staff are persons of integrity.

(e) Reporting lines of the internal audit function

Principle 12: The internal audit function should report to the audit committee or the board of directors and should inform senior management about its findings.

53. The Internal audit function is accountable to the board and its audit committee on all matters related to the performance of its mandate as described in the internal audit charter.

54. Senior management is responsible for implementing and maintaining an adequate and effective internal control framework. Therefore the internal audit function should inform senior management of all significant findings so that corrective actions can be taken. Subsequently, the internal audit function should follow up on the outcome of these corrective measures. The head of the internal audit function should report to the board, or its audit committee, the status of findings that have not (yet) been rectified by senior management.

(f) The relationship between the internal audit, compliance and risk management functions

Principle 13: Internal audit should both complement and assess operational management, risk management, compliance and other control functions.

55. The Committee's document about corporate governance explicitly mentions that a bank should have a risk management function, a compliance function and an internal audit function. Each of these control functions, along with the bank's operational management, constitutes a line of defence against the risks the entity faces[6]:

- 1st line Operational management
- 2nd line Risk management function, compliance function and other monitoring functions
- 3rd line Internal audit function

56. Control failings by one line of defence should, in principle, be detected by another line of defence. However, responsibility for internal control does not transfer from one line to another.

57. Operational management has ownership, responsibility and accountability for identifying, assessing, controlling, mitigating and reporting on risks encountered in the course of a bank's business activities.

58. The risk management function facilitates and monitors the implementation of effective risk management practices by operational management. It assists operational management in defining risk exposures and reporting through the organisation. The compliance function monitors the risk of non-compliance with laws, regulations and standards. These functions are also control functions which ensure that policies and procedures with regard to risk-taking are enforced. Other monitoring functions may include human resources and the legal department.

59. The internal audit function employs a risk-based approach to assess the efficiency and effectiveness of the design and operation of internal control and periodically provides assurance to senior management and the board of directors.

6. Internal audit within a group or holding company structure

Principle 14: The internal audit function in a group structure or holding company structure should be established centrally by the parent bank.

60. In a group structure, the board of directors and senior management of the parent company have the overall responsibility for ensuring that an adequate and effective internal audit function is established across the group and for ensuring that internal audit policies and mechanisms are appropriate to the structure, business activities and risks of all of the components of the group.

61. The parent bank should define the group's internal audit strategy, determine the organisation of the internal audit function both at the parent and subsidiary entity, formulate

---

[6] The concept of three lines of defence is also used in the Committee's *Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches,* June 2011

the internal audit principles, and determine the audit scope for the group. In doing so, it should comply with local legal and regulatory provisions and incorporate local knowledge and experience.

62. Principle 6 and related paragraphs of this document are also applicable to groups, that is, every activity (including outsourced activities) and every entity of the group should fall within the overall scope of the internal audit function.

7. Outsourcing of internal audit activities

Principle 15: Regardless of whether internal audit activities are outsourced, the board of directors remains ultimately responsible for ensuring that the system of internal control and the internal audit function are adequate and operating effectively.

63. It is recommended that large banks and internationally active banks perform internal audit activities using their own staff. However, outsourcing of internal audit activities on a limited and targeted basis can bring significant benefits to banks such as access to specialised expertise and knowledge for an internal audit engagement where the expertise is not available within the internal audit function. Outsourcing could also alleviate temporary resourcing constraints which might otherwise jeopardise the execution of the audit plan. Banks should be able to explain the reasons for outsourcing specific internal audit activities.

64. The head of internal audit should ensure that outsourcing suppliers comply with the principles in the bank's internal audit charter. To preserve independence, it is important to ensure that the supplier has not been previously engaged in a consulting engagement in the same area within the bank unless a reasonably long "cooling-off" period has elapsed. Similarly, as a best practice banks should not outsource internal audit activities to their own external audit firm[7].

65. The head of internal audit should ensure that, whenever practical, the relevant knowledge input from an expert is assimilated into the organisation. This may be possible by having one or more members of the bank's internal audit staff participate in the external expert's work.

B. The relationship of the supervisory authority with the internal audit function

66. The supervisory authority will benefit from effective communication about topics of mutual interest with the internal audit function of a bank. When establishing a relationship with the internal audit function of a bank, the supervisory authority should obtain an understanding of the organisation and operation of the internal audit function, including its position and remit within the bank.

67. Supervisors and internal auditors should each ensure that enhanced communication does not undermine their respective perceived and actual independence and status, as the supervisory authority and the internal audit function each have different roles and

[7] Any departure from this best practice should be limited to small banks and should remain within the bounds of the applicable ethical standards for the statutory or external auditor.

responsibilities. Regardless of the supervisor's assessment of the internal audit function, the supervisor should be able to challenge the work of the internal auditors through their continuous supervision process, including through on-site supervision.

68. The relationship between the supervisor and the internal audit function should be established in a structured and transparent way. In principle, the supervisor will initiate this relationship.

1. Benefits of enhanced communication between the supervisory authority and the internal audit function

Principle 16: Supervisors should have regular communication with the bank's internal auditors to (i) discuss the risk areas identified by both parties, (ii) understand the risk mitigation measures taken by the bank, and (iii) monitor the bank's response to weaknesses identified.

69. The internal audit function is a key building block of the internal control framework. Therefore, supervisory authorities have an interest in engaging in a constructive and formalised dialogue with the internal audit function. This dialogue could be a valuable source of information on the quality of the internal control framework.

70. The extent to which the work of internal auditors is factored into the supervisory course of action for a bank will depend on the supervisory approach, the supervisor's assessment of the internal audit function, and the circumstances relating to the issues at hand.

71. Supervisory authorities should receive periodically (e.g., on an annual basis), or upon request, the main internal audit findings and recommendations as well as the corrective measures taken or to be taken in response to the weaknesses identified, in the same way the audit committee is informed. Supervisors may request further information from internal auditors and require specific reports from time to time. The analysis of these internal audit reports and information may contribute to the supervisor's assessment of the internal control framework of the bank.

72. In addition to receiving reports, supervisory authorities should meet periodically with the bank's internal auditors to discuss their findings and recommendations. These meetings can also facilitate the understanding of how and to what extent the recommendations made by supervisors (including those made during on-site reviews) and internal auditors have been implemented. These meetings should be sufficiently frequent to enable the supervisor to ensure the effectiveness of the actions taken by the bank to carry out these recommendations. The frequency of these meetings and other communication between supervisors and internal auditors should be commensurate with the bank's size, the nature and risks of its operations and the complexity of its organisation.

73. Whenever there is a divergence from the internal audit plan, supervisors should obtain an understanding of the circumstances which led to the changes. Supervisors should also discuss the audit plan for the forthcoming year to ascertain whether the most sensitive risk areas are appropriately covered. In this respect, the audit committee's chair would be the appropriate person to be contacted by the supervisors.

74. The relationship between supervisors and internal auditors is also two-way. Supervisory authorities may consider sharing relevant information with the internal audit function when this could increase the effectiveness of the internal audit work and making

specific recommendations to strengthen the internal audit function, thereby strengthening the control environment.

2. Potential topics for discussion between supervisors and internal audit

75. Although all matters covered by the internal audit function are potentially of value to supervisors, some topics are closely related to supervisory requirements and are therefore of particular interest to banking supervisors.

76. A bank's capital and liquidity positions and its processes and methods for determining, monitoring, controlling and reporting on material risks are of direct relevance to supervisors. Therefore, supervisors and internal auditors should discuss the areas described in Section A - Principle 7 and related paragraphs.

77. Internal audit is well placed to provide the supervisor with insight on the institution's business model including risks in the institution's business activities, processes and functions and the adequacy of the control and oversight of these risks such as:

(i) Application and effectiveness of risk management procedures and risk assessment methodologies, as applied to credit risk, market risk, liquidity risk, operational risk (including information technology and business continuity management), and other risks relevant to the Basel capital adequacy Pillar 2 requirements;

(ii) Contingency planning;

(iii) Outsourcing arrangements; and

(iv) Fraud risk.

78. To the extent that accounting data drives certain regulatory measures or is included in regulatory reporting, supervisors should seek to understand and benefit from work performed by internal audit relating to:

(i) Measurement (including fair values) and impairment of financial instruments;

(ii) Significant transactions in financial instruments with a regulatory impact; and

(iii) Other judgemental accounting areas, including estimates.

79. Supervisors may also have an interest in business or market conduct issues as identified through the audit of the compliance function, for example:

(i) Transaction reporting;

(ii) Adherence to rules for dealing with client assets;

(iii) Anti-money laundering processes and controls; and

(iv) Management of conflicts of interest.

80. The board of directors and senior management are responsible for establishing the bank's strategy and business models. However, changes therein may have consequences for the bank's internal control, risk management and governance. Although internal audit does not set the bank's policies and should not interfere in its business decisions, it can be in a position to influence them by challenging management. Both the internal audit function and banking supervisors have an interest in the following:

(i) Processes for objective setting and strategic decision making; and,

(ii) Quality and substance of management and governance structure and processes.

C. Supervisory assessment of the internal audit function

81. Because of the crucial role played by internal audit in assessing the effectiveness of a bank's overall control functions, supervisors should assess the internal audit function. This will influence their overall assessment of the bank and enable them to determine the extent to which they will use of the work of the internal audit function.

1. Assessment of the internal audit function

Principle 17: Bank supervisors should regularly assess whether the internal audit function has an appropriate standing within the bank and operates according to sound principles.

82. The supervisory authority should consider the extent to which the board of directors, its audit committee and senior management promote a strong internal control environment supported and assessed by a sound internal audit function.

83. The assessment of the internal audit function should be based on the supervisory expectations as set out in section A of this guidance. This includes:

- The basic features of the internal audit function;
- The existence and content of the internal audit charter;
- The scope of the internal audit function's work;
- The corporate governance arrangements that apply to the internal audit function;
- The organisation of the function within a group or holding company;
- The remuneration structure of the head of the internal audit function and the key internal auditors; and
- Outsourced internal audit activities, if any.

84. In order to promote consistency and comparability over time and across banks and to identify industry best practices, the supervisory authority may benefit from using a grading system to perform its assessment of the internal audit function.

85. Weaknesses identified in the internal audit function may affect the supervisor's assessment of the bank's risk profile.

86. While the supervisory authority will independently assess the quality of the internal audit function, the audit committee or its equivalent and the internal audit function should develop and maintain their own tools to assess the quality of the internal audit function.

87. The appointment and replacement of the head of the internal audit function is relevant to the supervisory assessment of the bank. Therefore, the supervisory authority should be promptly informed by the audit committee (or its equivalent) or senior management of the appointment of a new head of the internal audit function, including relevant qualifications and previous experience. Similarly, whenever the head of the internal audit function ceases to act in this capacity the supervisory authority should be informed of this fact and its circumstances. The supervisory authority should consider meeting with the former head of internal audit to discuss the reasons for his or her departure.

2. Actions to be undertaken by the supervisory authority

Principle 18: Supervisors should formally report all weaknesses identified in the internal audit function to the board of directors and require remedial actions.

88. When the supervisory authority concludes that a bank's internal audit function is inadequate or ineffective, it should require the board of directors to develop an appropriate remedial plan that will restore the internal audit function to good standing on a timely basis. The plan should be communicated in writing to the supervisory authority for review. When the supervisor is not satisfied, it should require changes or additional measures to be included in the plan. The supervisor should monitor the implementation of the plan.

89. In addition to measures relating to the performance and standing of the internal audit function, the supervisor may also recommend enhancements to the governance of the bank including the functioning of the audit committee.

90. The audit committee and board of directors should not conclude that the internal audit function is functioning well solely because the supervisory authority has not identified weaknesses. The supervisory review process is not a substitute for the audit committee's assessment of or an external assessment of the internal audit function.

Principle 19: The supervisory authority should consider the impact of its assessment of the internal audit function on its assessment of the bank's risk profile and on its own supervisory work.

91. The assessment of the internal audit function may have consequences for the supervisor's assessment of the bank's risk profile, the allocation of supervisory resources and activities envisaged by the authority.

92. Where remedial actions cannot be agreed upon or where the bank faces ongoing delays in remediating the identified weaknesses, the supervisory authority should consider the impact of this on the bank’s risk profile.

93. In cases where a bank belongs to an international group, the supervisor should consider sharing its concerns with the other relevant authorities, for example within the supervisory college.

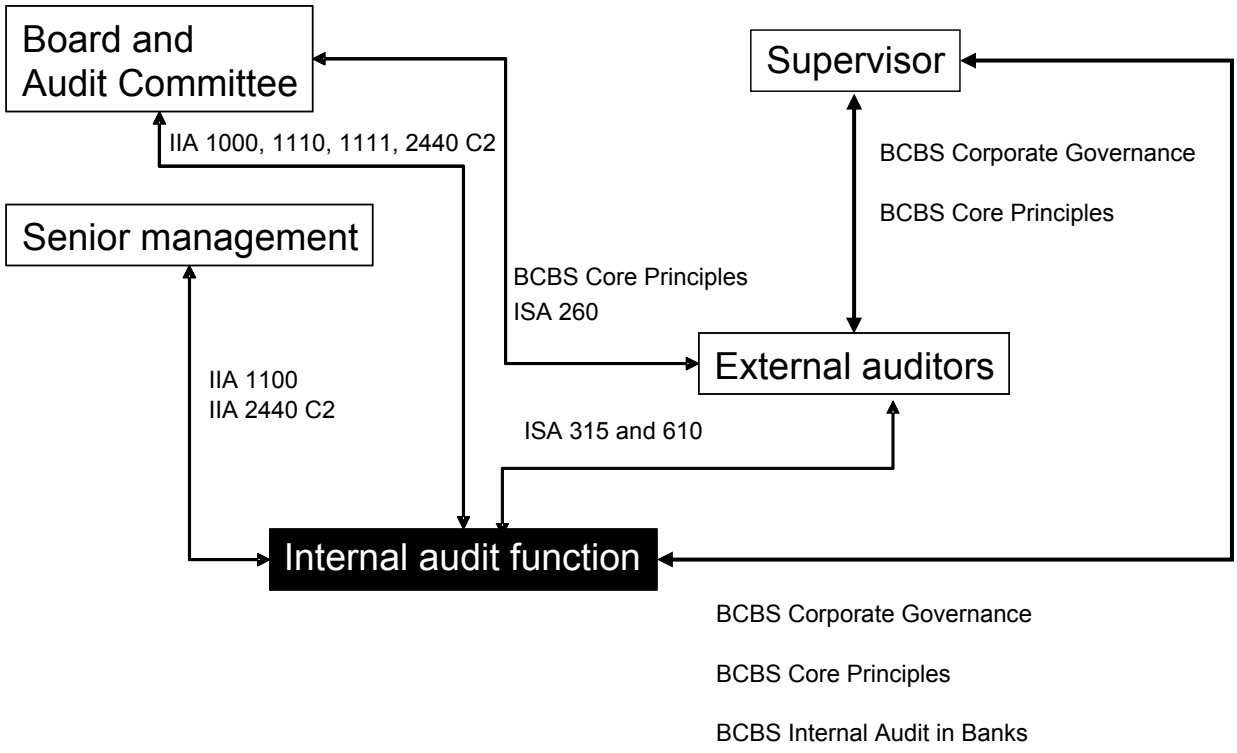
Principle 20: The supervisory authority should be prepared to take informal or formal supervisory actions requiring senior management and the board to remedy any identified deficiencies related to the internal audit function within a specified timeframe and to provide the supervisor with periodic written progress reports.

94. While supervisors expect banks to have a strong and robust internal audit function, there may be certain circumstances in which deficiencies exist and warrant specific supervisory actions aiming at remedying the deficiencies. Supervisory action may be of a public or non-public nature.

Annex 1

Internal audit function's communication channels

References to support these communication channels for the internal audit function are provided in the Committee's Core Principles and other relevant guidance issued by the Committee, International Standards on Auditing (ISAs) issued by the International Auditing and Assurance Standards Board, and the standards of The Institute of Internal Auditors (The IIA) as indicated. The diagram does not reflect all of the communication channels for parties other than the internal audit function.



- Basel Committee on Banking Supervision:
  - Core Principles for Effective Banking Supervision, October 2006
  - Principles for Enhancing Corporate Governance, October 2010
  - The Internal Audit Function in Banks, xxx 2012
- IIA: International Standards for the Professional Practice of Internal Auditing. Standards starting at 1xxx are Attribute Standards and Standards starting at 2xxx are Performance Standards. See International Professional Practices Framework (IPPF), The Institute of Internal Auditors, Altamonte Springs, Florida, USA, 2011.
  - IIA 1000 - Purpose, Authority, and Responsibility
  - IIA 1100 - Independence and Objectivity

  - IIA 1110 - Organizational Independence
  - IIA 1111 - Direct Interaction with the Board
  - IIA 2440 - Disseminating Results

- ISA: International Standards on Auditing. Standards starting at 2xx deal with the overall objectives and responsibilities of the external auditor, standards starting at 3xx deal with risk assessment and response to assessed risk by the external auditor and standards starting at 6xx deal with the external auditor's use of the work of others. See Handbook of International Quality Control, Auditing, Review, Other Assurance, and related Services Pronouncements, 2010 Edition Part 1, International Federation of Accountants, New York, New York, USA.
  - ISA 260 - Communication with Those Charged with Governance
  - ISA 315 - Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment
  - ISA 610 - Using the Work of Internal Auditors

Annex 2

Responsibilities of a bank's audit committee

The audit committee is a specialised committee within the board of directors. As such, it prepares the work of and reports to the board of directors in specific areas for which it has designated responsibility. The board of directors assumes final responsibility.

The main areas of responsibility of the audit committee are listed below by broad categories. The list provides a summary of sound practices for the audit committee of a bank. This list may vary according to local regulations and practices. For example, the responsibilities of an audit committee may be assumed directly by the board of directors in some banks or in some countries.

Financial reporting, including disclosures

(a) monitoring the financial reporting process and its output;

(b) overseeing the establishment of accounting policies and practices by the bank and reviewing the significant qualitative aspects of the bank's accounting practices, including accounting estimates and financial statement disclosures;

(c) monitoring the integrity of the bank's financial statements and any formal announcements relating to the bank's financial performance;

(d) reviewing significant financial reporting judgments contained in the financial statements; and

(e) reviewing arrangements by which staff of the bank may confidentially raise concerns about possible improprieties in matters of financial reporting.

Internal control

(f) ensuring that senior management establishes and maintains an adequate and effective internal control framework. Such framework should be designed to provide assurance in areas including reporting (financial, operational, risk), monitoring compliance with laws, regulations and internal policies, efficiency and effectiveness of operations and safeguarding of assets.

Internal audit

(g) monitoring and reviewing the effectiveness of the bank's internal audit function;

(h) approving the internal audit plan, scope, cycle (if any) and budget;

(i) reviewing and discussing internal audit reports;

(j) ensuring that the internal audit function maintains open communication with senior management, external auditors, the supervisory authority, and the audit committee;

(k) reviewing discoveries of fraud and violations of laws and regulations as raised by the head of the internal audit function;

(l) approving the audit charter and the code of ethics of the internal audit function;

(m) approving, or recommending to the board for its approval, the annual remuneration of the internal audit function as a whole, including the head of the internal audit function;

(n) reviewing the assessment by senior management of the head of the internal audit function and of the key internal auditors; and

(o) approving, or recommending to the board for its approval, the appointment, re-appointment or removal of the head of the internal audit function and the key internal auditors.

The statutory or external auditor

Appointment, reappointment, dismissal and remuneration

(p) approving a set of appropriate objective criteria for approving the statutory auditor or external audit firm of the bank;

(q) approving, or recommending to the board or shareholders for their approval, the appointment, re-appointment and removal of the statutory auditor or external audit firm;

(r) approving the remuneration and terms of engagement of the statutory auditor or external audit firm.

Compliance with relevant ethical requirements, in particular independence and objectivity

(s) reviewing and monitoring the independence of the statutory auditor or external audit firm, and in particular the provision of additional services to the bank, including the related safeguards that have been applied to eliminate identified threats to independence or reduce them to an acceptable level;

(t) reviewing and monitoring the statutory auditor's objectivity and the effectiveness of the audit process;

(u) developing and implementing a policy on the engagement of the statutory auditor or external audit firm for the supply of non-audit services, taking into account relevant ethical guidelines on the provision of non-audit services by the external audit firm; and

(v) Approving the total fees charged for the audit of the financial statements and for non-audit services provided by the external audit firm and external audit network firms to the entity and its components controlled by the entity.

The statutory audit or external audit

(w) overseeing the statutory audit of the annual and consolidated accounts;

(x) discussing with the statutory auditor or external audit firm key matters arising from the statutory audit or external audit, and in particular any identified material weaknesses in internal control in relation to the financial reporting process; and

(y) discussing the written representations the statutory auditor or external audit firm is requesting from senior management and, where appropriate, those charged with governance;

Remedial actions

(z) ensuring that senior management is taking necessary corrective actions to address the findings and recommendations of internal auditors and external auditors in a timely manner;

(aa) addressing control weaknesses, non-compliance with policies, laws and regulations and other problems identified by internal auditors and external auditors, and

(bb) ensuring that deficiencies identified by supervisory authorities related to the internal audit function are remedied within an appropriate time frame and reporting to the board of directors on the progress of necessary corrective actions.