Statement of Guidance

Internal Audit – Banks

1. Statement of Objectives

1.1. To provide specific guidance on one aspect of the requirement imposed on licensees by Rule 1(A).

1.2. To provide a standard of best practice to banks for the implementation of an effective and sound Internal Audit Function.

2. Introduction

Internal audit is part of the ongoing monitoring of the bank's system of internal controls and of its internal capital assessment procedure. 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.

3. Scope of an Internal Audit Function

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

a) the examination and evaluation of the adequacy and effectiveness of the internal control systems;

b) the review of the application and effectiveness of risk management procedures and risk assessment methodologies;

c) the review of the management and financial information systems, including the electronic information system and electronic banking services;

d) the review of the accuracy and reliability of the accounting records and financial reports;

e) the review of the means of safeguarding assets;

f) the review of the bank's system of assessing its capital in relation to its estimate of risk;

g) the appraisal of the economy and efficiency of the operations;

h) the testing of both transactions and the functioning of specific internal control procedures;

i) the review of the systems established to ensure compliance with legal and regulatory requirements, codes of conduct and the implementation of policies and procedures;

j) the testing of the reliability and timeliness of the regulatory reporting; and

k) the carrying-out of special investigations.

3.2. 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.

4. Permanent Function – Continuity

4.1. Each bank should have a permanent internal audit function in order to fulfil 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.

4.2. 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.

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

4.4. The application of this principle in the case of a group is discussed under section 9.

5. Independent function

5.1. 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.

5.2. 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 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).

5.3. 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. This reporting may cover, for example, bank management's making decisions, which are contrary to legal or regulatory provisions.

5.4. 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. An independent party such as an external auditor can carry out this review, or it can be done by the audit committee, if one exists.

6. Impartiality

6.1. 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.

6.2. 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.

6.3. 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.

6.4. 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. 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.

7. Audit charter

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

7.2. An internal audit charter establishes at least:

a) The objectives and scope of the internal audit function;

b) The internal audit department's position within the organisation, its powers, responsibilities and relations with other control functions; and

c) The accountability of the head of the internal audit department.

7.3. 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.

7.4. 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.

7.5. 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.

7.6. The charter should be communicated throughout the organisation.

8. Professional competence

8.1. 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.

8.2. 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.

8.3. 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.

8.4. 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.

8.5. 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.

9. Scope of activity

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

9.2. 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.

9.3. 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.

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

a) The bank's compliance with policies and risk controls (both quantifiable and non-quantifiable);

b) The reliability (including integrity, accuracy and comprehensiveness) and timeliness of financial and management information;

c) The continuity and reliability of the electronic information systems; and

d) The functioning of the staff departments.

9.5. 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 Monetary 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.

9.6. 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.

9.7. 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.

9.8. 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.

9.9. For branches abroad as well as for subsidiaries, the parent bank should establish the internal auditing principles centrally 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.

9.10. 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.

10. The bank's internal capital assessment procedure

10.1. 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.

10.2. 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.

10.3. 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.

10.4. 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.

11. Functioning of internal audit

11.1. Working methods and types of audit

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

11.1.1 There are different types of internal audit, which may include but are not limited to:

a) The financial audit, the aim of which is to assess the reliability of the accounting system and information and of resulting financial reports;

b) 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;

c) 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

d) 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.

11.1.2 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.

11.2. Risk focus and audit plan

11.2.1 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.

11.2.2 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.

11.2.3 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.

11.3. Procedures

11.3.1 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.

11.3.2 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.

11.3.3 A written audit report of each assignment is to be issued as quickly as possible. It is transmitted to the division audited and its management, and – in principle, in executive summary form – to senior management.

11.3.4 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.

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

11.3.6 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.

11.3.7 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).

11.4. Management of the internal audit department

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

11.4.2 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 the department's staff. The head of internal audit must continuously ensure the professional competence and training of the department's staff and that the necessary resources are available. Attention should be given to the staff's motivation and to its quality consciousness.

11.4.3 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.

12. Audit Committee

12.1. Definition

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 importance may, however, vary across entities.

12.2. 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. An audit 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.

12.3. Composition, powers and functioning

12.3.1 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.

12.3.2 An audit committee should include at least one member of the board of

directors. It is at the discretion of the bank to appoint the most appropriate individuals to serve as the other members of the committee. The members should have a background that is compatible with committee duties. 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.

12.3.3 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.

12.4. Relevant aspects

12.4.1 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 Monetary Authority.

12.4.2 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.

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

12.4.4 The audit committee regularly discusses:

a) The functioning of the internal control system;

b) The activities of the internal audit department;

c) Risk areas of the institution's operations to be covered in the scope

of the internal and external audits that year;

d) The reliability and accuracy of the financial information provided to management and external users;

e) Any material accounting or auditing concerns identified as a result of the external or internal audits; and

f) 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.

12.4.5 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.

13. Outsourcing

13.1. Definition

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

13.1.1 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,

13.2. Outsourcing of the internal audit

13.2.1 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.

13.2.2 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.

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

13.2.4 It would be ideal for the outsourcing vendor to be in all respects completely independent of the external auditor or of the latter's firm and group, however this may not be achievable in some instances. The Monetary Authority will consider, on a case-by-case basis, instances whereby outsourcing arrangements are 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 are encouraged to choose fully independent outsourcing vendors.

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

13.2.6 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.

13.2.7 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.

13.2.8 The contract should also state that senior management or its representative(s), the external auditor(s) or its representative(s), and the Monetary 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.

13.2.9 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.

13.2.10 When an institution enters into an outsourcing arrangement, it increases its operating risks. A bank is expected 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.

13.3. Outsourcing of internal audit activities in small banks

13.3.1 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 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.

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

14. General Guidance

This Guideline has been developed using *Internal audit in banks and the supervisor's relationship with auditors, August 2001* issued by the Basel Committee on Banking Supervision. For further guidance, institutions should consult papers issued by the Basel Committee on Banking Supervision, and the regulatory manuals from other internationally recognised regulators such as the Comptroller of the Currency (OCC), the Federal Reserve, and the Financial Services Authority (FSA).