Internal Audit in banks[1]

Directive by virtue of section 15 of the State Ordinance on the Supervision of the Credit System on the Internal Audit in banking organizations.

1. General

Within the meaning of this directive internal audit is defined as "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".

Adequate internal controls within banking organizations must be supplemented by an effective internal audit function that independently evaluates the control systems within the organization. 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.

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 analyze 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.

The principles discussed below should be followed when designing and implementing internal audit in banking organizations.

2. 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.

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

[1] This directive is largely based on the paper 'internal audit in banks and the supervisory relationship with auditors' issued by the Basel Committee on Banking Supervision in August 2001.

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.

Senior management should maintain an organizational 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. The risk management process must also include a systematic analysis of integrity risks, as defined in the Directive on Sound Business Operations. Reference is made to article 7 of the Directive on Sound Business Operations. 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.

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.

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.

3. Principles of internal audit

3.1 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.

Only in very exceptional cases (e.g. if due to the size of a bank the establishment of an own internal audit department is not economically feasible) it is allowed to outsource this function to a third party vendor other than the bank's own external auditor. Senior-Management and Board of Directors remain also in such cases fully responsible for the adequacy and effectiveness of the internal audit function. In case the necessary expertise for parts of the audit to be performed is not available inhouse, a bank can hire outside vendors other than the bank's own external auditor to execute part of the audit work.

3.2 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.

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.

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.

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.

3.3 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.

An internal audit charter establishes at least:

- the objectives and scope of the internal audit function;

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

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 also provide this confirmation.

In the charter, the bank's senior management gives the internal audit department the right of initiative and authorizes 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.

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 and should be communicated throughout the organization.

3.4 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.

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.

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.

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 reorganizations, the start of important or risky new activities, new establishments which are to carry out risky activities, and the setting up or reorganization 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.

3.5 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.

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.

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.
Continuously performing similar tasks or routine jobs may negatively affect an internal auditor's capacity for critical judgment. 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 jeopardize the independence of the internal auditors.

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.

3.6 Scope of activity

Principle 9
Every activity and every entity of the bank should fall within the scope of the internal audit.

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.

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.

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.

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 organized and managed. However, this does not imply that the internal audit department should assume the compliance function.

3.7 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.

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 maximize the risk/reward trade-off within the different areas of the bank.

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.

4. Functioning of internal audit

4.1 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 on recommendations and issues.

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 analyze the organizational 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.

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.

4.2 Risk focus and audit plan

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.

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.

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.

4.3 Procedures

For each audit assignment an audit program should be prepared. The audit program describes the objectives as well as an outline of the audit work that is considered necessary to achieve them.

All audit procedures forming part of the assignment should be documented in working papers. These must reflect the examinations that have been made and emphasize 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.

A written audit report of each assignment is to be issued as quickly as possible. It is transmitted to the auditee and to senior management.

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.

The internal audit department follows up on 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).

4.4 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.

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.

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 organization 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.

4.5 The relationship of the internal auditors and the external auditors

Principle 13

There should be regular consultation between internal and external auditors in order to make their cooperation as efficient and effective as possible.

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.

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.

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.