Attachment to the BSD Circular No. 07 dated May 27, 2004.

STATE BANK OF PAKISTAN

BANKING SUPERVISION DEPARTMENT

Guidelines on Internal Controls

State Bank of Pakistan, 5th Floor, Main Building, I. I. Chundrigar Road, Karachi

Index

1 Introduction

Internal Control refers to policies, plans and processes *as* affected by the board of directors and performed on continuous basis by the senior management and all levels of employees within the bank. These internal controls are used to provide reasonable assurance regarding the achievement of organizational objectives. The system of internal controls includes financial, operational and compliance controls.

While safeguarding the organization's assets, internal controls primarily aim to support the management in the identification and mitigation of those risks which the organization may encounter in the fulfillment of business objectives of an organization.

An internal control system encompasses the policies, processes, tasks, behaviors and other aspects of a company that, taken together: facilitate its effective and efficient operation by enabling it to respond appropriately to significant business, operational, financial, compliance and other risks to achieving the company's objectives. This includes the safeguarding of assets from inappropriate use or from loss and fraud, and ensuring that liabilities are identified and managed; help ensure the quality of internal and external reporting. This requires the maintenance of proper records and processes that generate a flow of timely, relevant and reliable information from within and outside the organization; and help ensure compliance with applicable laws and regulations, and also with internal policies with respect to the conduct of business.

With regard to banking sector, a system of effective internal controls strengthens the base of safe and sound banking. Therefore, a properly designed and effectively enforced system of internal controls helps protect organization's assets and profitability, produces reliable financial reports, ensures compliance with laws and regulations, and finally, safeguards interest of the stakeholders. Effective internal control also reduces the possibility of significant errors, lapses and irregularities and assists in their timely detection when they do occur.

In simple terms, Internal Controls provide an additional reference tool for all managers to identify and assess basic weaknesses in operating controls, financial reporting, and legal/regulatory compliance and to take action to strengthen controls where needed. By developing effective compliance programs, management can contribute to reducing the bank's potential liability from fines and penalties that could be imposed for violations.

It is well proven that there is strong complementarity between an effective risk management system and a sound internal controls system. However, it may be noted that vis-à-vis risk management concepts, the definition of internal controls stretches beyond the typical checks and balances and include effective and ongoing reviews of the risks. Understandably all risks may not be eliminated, however, an effective internal control system comes to help mitigate effectively many of the risks faced by an organization. That is, risks may be brought down within acceptable levels through an effective internal control system.

Through their experience of banking crisis, financial experts all over the world have learnt that major internal control failures, which cause significant losses to banks, can be avoided or at least controlled if the board and senior management of the organizations establish a strong control cultures. It has come to the fore that a weak control culture often has two common elements. First, senior management fails to emphasize the importance of a strong system of internal control through their words and actions. Second, senior management does not define, in clear terms, the organizational structure and managerial accountabilities.

State Bank of Pakistan has been persistently persuading the banks / DFIs to adopt robust risk management practices. As a part of our ongoing efforts we are issuing **Guidelines on Internal Controls.** These guidelines are issued with the objective of encouraging and helping banks/DFIs, from a supervisory perspective, in instituting an effective system of internal controls which is commensurate with the nature, complexity, and risk inherent in their activities and which responds to changes in the environment and conditions the banks/DFIs work in.

These guidelines apply to all the banks / DFIs. The control activities contained in this guide are not presented as all-inclusive or exhaustive of all the specific controls appropriate in each department / activity of banks / DFIs. Over time, controls may be subject to change to reflect changes in our operating environment. Further, we believe that internal controls are established to manage the risk of failure to meet business objectives and to provide reasonable assurance against material mis-statement or loss. In fact, internal controls refer to a process; a mean to an end, not an end in themselves.

1.1 Objectives of Internal Controls

Objectives of internal controls are to help bank management evaluate processes, assess their performance and manage risks. Good internal controls can help a bank achieve its objectives and avoid surprises.

Every system is run by human beings who, by the very nature, are vulnerable to personal distraction, carelessness, fatigue, errors in understanding and judgment, or unclear instructions in addition to fraud or deliberate noncompliance with policies. Effective controls systems help detect such mistakes, thus help rectify them before its too late.

Broad objectives of Internal Controls include:

- To ensure efficiency and effectiveness of operations;
- To ensure reliability, completeness and timeliness of financial and management information; and
- To ensure compliance with policies, procedures, regulations and laws.

The ***performance*** objectives are focused on assets protection, operational efficiency and risk management; the ***information*** objective of the internal controls target accuracy of recording and adequacy of disclosure. Lastly, ***compliance*** objective of internal controls is meant to ensure adherence to laws, regulations and internal polices relevant to the organization.

In general, internal controls are simply good business practices, adequate checks and balances, and include anything which serves to safeguard bank's assets and to improve the effectiveness and efficiency of operations.

All banks / DFIs need to ensure that there exist; an organizational structure that establishes clear lines of authority and responsibility for monitoring adherence to prescribed policies; effective risk assessment framework; timely and accurate financial, operational, and statutory disclosure; adequate set of procedures to safeguard and manage assets and; system of compliance with applicable laws and regulations.

An effective internal control system requires that the material risks that could adversely affect the achievement of the bank's goals are being recognized and continually assessed. This assessment should cover all risks facing the bank and the consolidated banking organization (that is, credit risk, market risk, liquidity risk, operational risk, country risk and reputation risk etc.). Internal controls may need to be revised to appropriately address any new or previously uncontrolled risks.

2 Control Principles

Lessons learnt from the history of banking crisis can be enumerated in the form of widely accepted and well-tested 'Controls Principles' and need to be followed by all organizations, irrespective of size, nature and complexity of their business, while developing framework of internal controls. These principles include following;

<u>Cover all activities</u>: All banks should develop internal controls which have coverage over all their functions, in general, and the key risk areas (KRA)[1], in particular.

<u>Regular feature</u>: Control activities should be an integral part of the daily activities of a bank / DFI in such a manner that it becomes ingrained in their ongoing processes rather than a year-end "fire drill" to satisfy documentation requests from auditors and supervisors.

<u>Separation of Duties</u>: Duties should be divided so that no one person has complete control over a key function or activity.

[1] Key Risk Areas include those core activities, the break down of which may render a bank unable to meet its obligations; to its customers, regulators and the sponsors. Further, the risk originating from such activities is of the type that it may cause in systemic failure of other financial institutions. Examples of key risk areas are Liquidity Risk, Interest Rate Risk, Foreign Exchange Risk, Credit Risk, Operational Risk, etc.

Authorization and Approval: All transactions should be authorized before recording and execution.

Custodial and Security Arrangements: Responsibility for custody of assets needs to be separated from the related record keeping.

Review and Reconciliation: Records should be examined and reconciled to regularly determine that transactions are properly processed, approved and booked.

Physical Controls: Equipment, inventories, cash and other assets should be secured physically, counted periodically and compared with amounts shown on control records.
Training and Supervision: Qualified, well-trained and supervised employees always help ensure that control processes function properly.

Documentation: Documented policies and procedures promote employee understanding of duties and help ensure continuity during employee absences or turnover. Therefore, policies and procedures (in the form of operations manuals and desk instructions) should exist in all banks / DFIs.

Communication of importance of Internal Controls: Setting standards of professional integrity and work ethics and ensuring that all levels of personnel in their organization know the importance of internal controls and understand their role in the internal controls process and be fully engaged in the process.

Cost/Benefit: It is for the banks to assess the costs associated with control processes commensurate with the expected benefits.

3 Components of Internal Control System

All banks / DFIs are required to establish a reliable system of internal controls which largely depends on a bank's size; nature, scope and complexity of its business; and the risk associated with its activities.

Internal control must be consistently applied and well understood by bank staff if board and management policies are to be effectively implemented.

An effective internal control system consists of following interrelated components:

a) Control environment;
b) Risk recognition and assessment;
c) Control activities and segregation of duties;
d) Accounting, information & communication; and

e) Self-assessment or monitoring and correcting deficiencies.

3.1 Control Environment:

The environment in which internal control operates has an impact on the effectiveness of the control procedures. In fact it is institution's control environment which embodies the principles of strong internal control. Besides giving structure to the internal control system, it provides discipline and protocol.

The success of control environment is judged according to; the integrity, ethics, and competence of personnel; the organizational structure of the institution; oversight by the board of directors and senior management; management's philosophy and operating style; attention and direction provided by the board of directors and its committees, especially the audit and risk management committees; personnel policies and practices and; external influences affecting operations and practices.

In order for internal controls to be effective, an appropriate control environment should demonstrate following behaviors:

- Board of directors reviews policies and procedures periodically and ensures their compliance;
- Board of directors determines whether there is an audit and control system in place to periodically test and monitor compliance with internal control policies/procedures and to report to the board instances of noncompliance;
- Board of directors ensure independence of internal and external auditors such that internal audit directly reports to the audit committee of the board which is responsible to the board and that external auditor interacts with the said committee and presents management letter to the board directly;
- Board ensures that appropriate remedial action has been taken when instance of noncompliance are reported and that system has been improved to avoid recurring errors/mistakes;
- Management information systems provides adequate information to the board and that the board can have access to bank's records, if need arises;
- Board and management ensure communication of conduct or ethics policies and compliance thereof down the line within the organization;

In short, a strong control environment and an effective internal audit function, can significantly complement specific control procedures. However, constitution of internal control environment at a point-of-time does not, by itself, ensure the effectiveness of the overall system of internal control but it is the continuous supervision by management to ensure if it is functioning as prescribed and is modified as appropriate.

3.2 Risk assessment and management:

Every banking activity involves some kind of risk and this creates a compulsion for the banks that, as part of an internal control system, these risks are being identified, assessed and mitigated. From an internal control perspective, risk assessment involves; identification and evaluation of factors, both internal[2] and external[3], that could adversely affect performance, information and compliance objectives of a bank. It may be noted that it differs from the risk management process, which typically focuses more on the review of business strategies and plans developed to maximize the risk/reward trade-off within the different areas of the bank.
This risk identification should be done across the full spectrum of activities addressing both measurable and non-measurable aspects of risks. Second part of risk assessment – evaluation – is done to determine which risks are controllable by the bank and which are not. For those risks that are controllable, the bank must assess whether to accept those risks or the extent to which it wishes to mitigate the risks through control procedures. For those risks that cannot be controlled, the bank must decide, for the present, whether to accept these risks or to withdraw from or reduce the level of business activity concerned. But for the future, internal controls may need to be revised to appropriately address any new or previously uncontrolled risks.

An effective risk assessment system allows the board and the management to plan for and respond to existing and emerging risks in the bank's activities. For that matter, such a system needs to demonstrate following:

- Board and management involve audit personnel or other internal control experts in the risk assessment and risk evaluation process. Those experts should be competent, knowledgeable, and provided with adequate resources.
- As the risks mutate with time and with changing circumstances, the board and the management, with due involvement of audit personnel, should appropriately evaluate the risks and consider control issues related to existing products and those relevant to new products and activities.
- Risk coverage in the form of insurance (that is risk transfer) or provisioning (contingency fund) in relation to the bank's risk profile is adequate.

3.3 Instituting Controls:

Control activities are designed and implemented to address the risk that the bank identified through the risk assessment process as described above. Control activities involve: (a) establishment of control policies and procedures, (b) verification that the control policies and procedures are being complied with.
It is desired that control activities should involve all levels of personnel in the bank, including senior management as well as front line personnel. Instituting an appropriate controls structure ensures the efficacy of an internal control system. This process involves;

---

[2] Internal factors include: complexity, nature and size of operations; quality of personnel and employee turnover; objectives and goals, etc.
[3] External factors include: fluctuating economic conditions, changes in the industry and technological advances, degree of aggressiveness of the market and competition faced by the market participants, etc.

- Existence and compliance of policies and procedures ensuring that decisions are made with appropriate approvals and authorizations for transactions and activities while assuring that exceptions to the policies are minimal and reported to the board and the top management;
- Timely reconciliation of accounts so that outstanding items, both on-and off-balance-sheet, are resolved and cleared;
- Segregation of duties, existence of cross-checks, more-than-one-person authorization, dual controls, joint custody of keys, safeguards for access to and use of sensitive assets and records and forced leave policies, employees rotation systems are functioning in sensitive positions or risk-taking activities so that concerned employees do not have absolute control over areas;
- Building of such reporting lines within a business or functional area that independence of the control function is ensured;
- Accountability mechanism for the actions taken by the personnel as per their responsibilities and authorities;
- Structure and functioning of compliance framework through which the board and senior management establishes that compliance with applicable laws and regulations is ensured. This includes board's and senior management's knowledge about audit schedules, scopes, and reports; recording of minutes of senior management and board committees and reporting of payment of any fines or liabilities arising from litigation against the institution or its employees. Board's and the senior management's demonstration of willingness and ability to prevent reoccurrence of significant and frequent violations are important in this regard.

In short, top level reviews; appropriate activity controls for different departments or divisions; physical controls; checking for compliance with exposure limits and follow-up on non-compliance; a system of approvals and authorizations; and, a system of verification and reconciliation are major constituents of the control activities.

3.4 Accounting, Information & Communication Systems:

An institution's accounting, information, and communication systems ensure that risk-taking activities are within policy guidelines and that the systems are adequately tested and reviewed. For this the following is important to note;

An ***accounting system*** is adequate if it properly identifies, assembles, analyzes, classifies, records, and reports the institution's transactions in accordance with prescribed formats and international best practices.

The adequacy of ***information systems***[4] is determined by the type, number, and depth of reports it generates for operational, financial, managerial, and compliance-related activities and

[4] The adequacy of information system means increased controls over computer systems, personal computers (PCs) and computer operations. The list of persons whose computers have access to assets or financial records is very important from internal control perspective; it includes computer operators, programmers, their supervisors, and others. Banks should impose sophisticated controls not only on mainframe operations but also on the systems and records maintained on PCs, local area networks (LANs), and wide area networks (WANs).

the access and authorization to information systems. An ideal information systems covers the full range of its activities in such a manner that information remains understandable and useful for audit trail.

On the one hand, the adequacy of ***communication systems*** is established by the fact that it imparts significant information throughout the institution (from the top down and from the bottom up, and laterally), ensuring that personnel understand whatever has been communicated and, on the other hand, communication system should ensure that significant information is imparted to external parties such as regulators, shareholders, and customers.

Furthermore, for ensuring adequacy and functionality, there should be frequent and thorough testing and verification of the accounting, information, and communication systems. It must be noted that risks inherent in the use of information technology; for accounting, information and communication purposes, should be controlled by banks in order to avoid disruptions to business.

3.5 Self-Assessment and Monitoring:

An integral component of internal control system is self-assessment and monitoring which includes;

- Board and senior management oversight of the internal control, control reviews, and audit findings. Before starting full scale control review, the board and senior management should give their approval of the overall scope of the control review activities (e.g., audit, loan review, etc.).
- Frequent and comprehensive reporting of deviations to the board or board committee and senior management regarding sufficiency of details and timely presentation to allow for resolution and appropriate action.
- Adequate[5] documentation of management responses to audit or other control review findings so that it can be tracked for adequate follow-up.
- Board or board committee or senior management review of the qualifications and independence of the personnel evaluating controls (e.g., external auditors, internal auditors, or line managers).

4 Responsibilities

The board of directors, senior management and other personnel of banks/DFIs are responsible for establishing, maintaining, and operating an appropriate internal control system on an ongoing basis.

[5] Here adequacy of documentation refers to detailing the coverage, findings, and follow-up of control weaknesses; appropriate and timely attention given by management to control weaknesses once identified and system of holding the line management accountable for unsatisfactorily or ineffectively following up on control weaknesses.

4.1 Board of Directors:

The Board of Directors of all banks/DFIs, is responsible for ensuring that an adequate and effective internal control system exists in their organization and that the senior management is maintaining and monitoring the performance of that system. Moreover, Board should periodically review the internal control systems and the significant findings.

4.2 Management:

Senior management of banks/DFIs have the responsibility for implementing strategies and policies as approved by the board; developing processes that identify, measure, monitor and control risks incurred by the bank; maintaining an organizational structure that clearly assigns responsibility, authority and reporting relationships; ensuring that delegated responsibilities are effectively carried out; setting appropriate internal control policies; and monitoring the adequacy and effectiveness of the internal control system.

4.3 Internal Auditor:

In addition to above, management shall entrust to the Internal Auditors, the supervisory functions with respect to the review of internal controls. Internal auditors shall evaluate and validate the effectiveness of control systems, monitor control systems, and contribute to ongoing effectiveness of control systems. The internal audit department shall produce, on quarterly basis, a report on internal control system and significant findings and present it to the Audit Committee of the Board.

4.4 External Auditor:

The external auditors are not part of a banking organization and, therefore, are not part of its internal control system, yet they have an important impact on the quality of internal controls through their audit activities, including discussions with management and recommendations for improvement to internal controls. The external auditors provide important feedback on the effectiveness of the internal control system.

The concept of external reporting on internal controls is well established and supported in the accounting literature. It is expected that external / statutory auditors shall review control systems for the impact they have on financial reporting and compliance with relevant policies, procedures, regulations and laws. The extent of attention given to the internal control system may vary by auditor and by bank; however, it is generally expected that the auditor would identify significant weaknesses that exist at a bank and report material weaknesses to management and the board / audit committee of the board in the form of an audit report / management letter.

4.5 Supervisor / Regulator:

During the course of regular inspection of banks/DFIs or when required, Banking Inspection department of State bank of Pakistan shall review the internal control system of all banks/DFIs in order to ensure compliance with these guidelines and all other relevant regulations and laws, issued and enforced from time to time. In addition to that, the SBP will review the report of the internal auditor of the banks / DFIs, assessment report of the management regarding effectiveness of the internal control and Boards' endorsement thereof and the external / statutory auditors' evaluation of the management regarding effectiveness of the internal control.

5 Implementation of Internal Controls:

Various models/methodologies are used for the design and implementation of internal controls. However, it is the decision of the organizations to decide what model / strategy suit the size, nature, complexity, scope, risk exposure, etc. of their activities. Nevertheless, following is a brief summary of the key points that should be kept in mind while implementing the internal controls:

a) **Compare current practices to the internal control system and identify gaps.** For an internal control expert, the most important consideration should be to evaluate the existing system of internal control in comparison to one defined by these guidelines and other international best practices. In this regard the first step is to identify what is and what is not covered by existing practices.

b) **Involve senior management, the audit committee, audit staff, other key players.** The thought process and implementation of change should not be considered as "just other audit things." Senior management and the audit committee must be perceived as driving the change and developing the control culture.

c) **Assess business environment, organization culture and key players.** Before the process of change is set in, it would be necessary to understand: (1) what is changing in the culture? (2) What is changing in the organization's businesses and systems? (3) Are there organizational initiatives which internal control system implementation could link to? (4) What is the perception about the internal auditing function within the organization?

d) **Decide on implementation strategy.** If the new practices can be designed to align with other organizational initiatives, or if senior management has taken ownership, this step is relatively easy. In any case, having a realistic implementation strategy is critical to success. Most implementers introduce the new ideas slowly and informally, building on personal relationships within the organization, listening as much as talking, and gradually building a consensus for change.

e) **Provide training to everyone involved.** The most critical factor to the successful implementation of a control model is that everyone involved must understand internal control. Effective training depends heavily on how concepts are phrased and the concrete examples and exercises which make the concepts real to participants.

f) **Rectification & Improvement:** The findings of the internal audit department and that of other experts should be reported back to the relevant staff/office for rectification and improvement of the internal control system.

6 Evaluation of Internal Controls

Effective and well-designed control systems are subject to execution risk. The employees implement the internal control system and even well trained personnel with the best of intentions can become distracted and negligent. Therefore, evaluation of internal controls is far more necessary so that intentional as well as unintentional mistakes and deviations from policies, procedure and laws are minimized. For that matter overall effectiveness of the bank's internal controls should be monitored on an ongoing basis. Monitoring of key risks should be part of the daily activities of the bank as well as periodic evaluations by the business lines and internal audit.

The whole evaluation philosophy revolves around following ideas:

- Identification of the internal control objectives that are relevant to the organization, unit or activity under review (e.g., lending, investing, accounting);
- Assessment of effectiveness of the internal control elements, not just by reviewing policies and procedures, but also by reviewing documentation, discussing operations with various levels of bank personnel, observing the operating environment, and testing transactions;
- Communication of the concerns of auditor / evaluator about internal controls and their recommendations for improvement to the board of directors and management on a timely basis, and;
- Assurance that, where deficiencies are noted, corrective action is taken in a timely manner.

6.1 Process of Evaluation of Internal Controls:

Evaluation of internal control involves;

1) Identifying the internal control objectives relevant to the bank, department, business line, or product;
2) Reviewing pertinent policies, procedures, and documentation;
3) Discussing controls with appropriate levels of bank personnel;
4) Observing the control environment;
5) Testing transactions as appropriate;
6) Sharing findings, concerns, and recommendations with the board of directors and senior management; and
7) Determining that the bank has taken timely corrective action on noted deficiencies.

The review of internal control consists mainly of enquiries of auditor/evaluator with reference to documentation such as procedures manuals, job descriptions and flow charts, to gain knowledge about the controls, which he/she has identified as significant to his/her audit/evaluation.

Different techniques, narrative descriptions, questionnaires and flow charts, are used to record information relating to an internal control system and selection of a particular technique is a matter for the auditor's judgment. However, the auditor should maintain adequate documentation about those internal controls on which he/she intends to rely.

Who should evaluate the efficacy of internal controls? Ideally, there should be an effective and comprehensive internal audit of the internal control system carried out by operationally independent, appropriately trained and competent staff. The internal audit function, as part of the monitoring of the system of internal controls, should report directly to the board of directors or its audit committee, and dotted line to senior management.

Besides internal audit's evaluation of internal controls, the external auditors, during the course of statutory audit, evaluate internal controls of the banks/DFIs. They normally express an opinion on the report of the board of directors of banks/DFIs on internal controls and their opinion becomes part of the annual financial disclosures by the banks/DFIs.

Management of all banks/DFIs should provide their internal audit departments, external auditors and SBP inspectors with adequate access to information in determining whether their organizations have a satisfactory system of the internal controls.

In reviewing internal control in a specific area of the bank, it is necessary to identify key control personnel and positions. Answers to following questions would help the evaluator in forming a view regarding soundness of the internal controls:

- What are the critical functions and who are the critical personnel[6] in an organization/department holding position relevant to that function?
- What if that person makes a significant error? For instance, in case of internal controls regarding financial disclosure, an inaccurate recording of transactions can distort all the analyses and decisions made on the basis of that information.
- If an error or irregularity occurs, would normal controls promptly detect it?
- Is it possible for a person to conceal an error or irregularity, and are there controls in place to minimize this possibility and if one has occurred then detect them promptly?
- Are employees' duties and responsibilities properly segregated to minimize the possibility of errors and irregularities?
- What are the circumstances that may cause bank employees or officers to take undue risks?
- Are internal controls sound enough to ensures that conflicts of interest are minimized or controlled?

Above list is not at all exhaustive. It is an attempt to give few examples of the type of questions which the auditor/evaluator must consider before reaching conclusions about a specific area's internal control.

[6] Personnel who have influence over financial records and access to assets. Persons in these positions could be involved in information processing (computer programmers) or investment and trading activities (traders, buyers, and sellers).

6.2 Communication of Weaknesses

Internal control deficiencies, whether identified by business line, internal audit, or other control personnel, should be reported in a timely manner to the appropriate management level and addressed promptly. Material internal control deficiencies should be reported to senior management and the board of directors. Such weaknesses are usually communicated in writing.

The report should speak about deviations by bank personnel from established policies, practices, and procedures. Such deviations exist when:

- Instructions/directives are not reviewed and revised regularly to reflect current practices.
- Employees use shortcuts to perform their tasks, circumventing internal control procedures.
- Changes in organization or activities are not promptly reflected in policies or procedures.
- Employees' duties are changed significantly in ways that may affect internal control policies.

Report should give fair assessment of their significance. Further, both manifest and potential conflicts of interest should be considered in the overall assessment and communication of internal control.

---

7 Reporting of Internal Controls

All banks/DFIs are required to include a 'Statement on Internal Controls' in their annual reports. That statement should include following:

a) A statement of management's responsibilities for establishing and maintaining adequate internal controls and procedures followed by management's evaluation of the effectiveness of the bank's internal controls;

b) Board of Directors' endorsement of the management's evaluation; and

c) Statutory Auditors' attestation to, and report on, Board's endorsement regarding efficacy of company's internal controls, which are relevant to the financial reporting only.

Management's evaluation of internal controls may include, but not limited to;

- A description of management's responsibilities for establishing and maintaining a system of internal control directly related to, and designed to provide reasonable assurance as to the integrity and reliability of those controls and reports produced there form;

- An assessment of the effectiveness of the company's system of internal control that encompassed material matters; and

- A statement of how management responded to any significant recommendations concerning its system of internal controls made by its internal as well as external auditors.

Major components of that statement may include, but not limited to:

1) It may include a narration as: For the year under review, it has been endeavored to follow the Guidelines on Internal Controls and that it is an ongoing process for the identification, evaluation and management of significant risks faced by the bank/DFI.

2) Keeping in view the risk exposure, internal controls are regularly reviewed and reported on their soundness.

3) The report may include the fact that Board of Directors is ultimately responsible for the internal control system. It may also include that such system is designed to manage, rather than eliminate the risk of failure to achieve the business objectives, and can only provide reasonable and not absolute assurance against material mis-statement or loss.

4) Where a BOD cannot make full review or that of one or more aspect of internal controls, it should state this fact and provide an explanation.

Annexure

Principles[7] for the Assessment of Internal Control Systems[8]

A) Management oversight and the control culture

Principle 1:

The board of directors should have responsibility for approving and periodically reviewing the overall business strategies and significant policies of the bank; understanding the major risks run by the bank, setting acceptable levels for these risks and ensuring that senior management takes the steps necessary to identify, measure, monitor and control these risks; approving the organizational structure; and ensuring that senior management is monitoring the effectiveness of the internal control system. The board of directors is ultimately responsible for ensuring that an adequate and effective system of internal controls is established and maintained.

Principle 2:

Senior management should have responsibility for implementing strategies and policies approved by the board; developing processes that identify, measure, monitor and control risks incurred by the bank; maintaining an organizational structure that clearly assigns responsibility, authority and reporting relationships; ensuring that delegated responsibilities are effectively carried out; setting appropriate internal control policies; and monitoring the adequacy and effectiveness of the internal control system.

Principle 3:

The board of directors and senior management are responsible for promoting high ethical and integrity standards, and for establishing a culture within the organization that emphasizes and demonstrates to all levels of personnel the importance of internal controls. All personnel at a banking organization need to understand their role in the internal controls process and be fully engaged in the process.

B) Risk Recognition and Assessment

Principle 4:

An effective internal control system requires that the material risks that could adversely affect the achievement of the bank's goals are being recognized and continually assessed. This assessment should cover all risks facing the bank and the consolidated banking organization (that is, credit risk, country and transfer risk, market risk, interest rate risk, liquidity risk, operational risk, legal risk and reputational risk). Internal controls may need to be revised to appropriately address any new or previously uncontrolled risks.

C) Control Activities and Segregation of Duties

Principle 5:

Control activities should be an integral part of the daily activities of a bank. An effective internal control system requires that an appropriate control structure be set up, with control activities defined at every business level. These should include: top level reviews; appropriate activity controls for different departments or divisions; physical controls; checking for compliance with exposure limits and follow-up on non-compliance; a system of approvals and authorizations; and, a system of verification and reconciliation.

[7] BIS Framework for Internal Control Systems in Banking Organizations

[8] All in all there are 13 Principles; however, the 13th Principle, which is relevant to the Supervisors only, has not been included in this annexure.

Principle 6:

An effective internal control system requires that there is appropriate segregation of duties and that personnel are not assigned conflicting responsibilities. Areas of potential conflicts of interest should be identified, minimized, and subject to careful, independent monitoring.

D) Information and communication

Principle 7:

An effective internal control system requires that there are adequate and comprehensive internal financial, operational and compliance data, as well as external market information about events and conditions that are relevant to decision making. Information should be reliable, timely, accessible, and provided in a consistent format.

Principle 8:

An effective internal control system requires that there are reliable information systems in place that cover all significant activities of the bank. These systems, including those that hold and use data in an electronic form, must be secure, monitored independently and supported by adequate contingency arrangements.

Principle 9:

An effective internal control system requires effective channels of communication to ensure that all staff fully understand and adhere to policies and procedures affecting their duties and responsibilities and that other relevant information is reaching the appropriate personnel.

E) Monitoring Activities and Correcting Deficiencies

Principle 10:

The overall effectiveness of the bank's internal controls should be monitored on an ongoing basis. Monitoring of key risks should be part of the daily activities of the bank as well as periodic evaluations by the business lines and internal audit.

Principle 11:

There should be an effective and comprehensive internal audit of the internal control system carried out by operationally independent, appropriately trained and competent staff. The internal audit function, as part of the monitoring of the system of internal controls, should report directly to the board of directors or its audit committee, and to senior management.

Principle 12:

Internal control deficiencies, whether identified by business line, internal audit, or other control personnel, should be reported in a timely manner to the appropriate management level and addressed promptly. Material internal control deficiencies should be reported to senior management and the board of directors.

****