Internal Control Policy

1. Introduction

An effective system of internal control is vital for the success of an organization, especially financial institutions that are entrusted with public money. The internal controls refer 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. The system of internal controls includes financial, operational and compliance controls. An internal control system includes the safeguarding of assets from inappropriate use or from loss and fraud, and ensuring that liabilities are identified and managed.

Internal control improvement is an ever evolving process and needs to complement change in the operating environment. Therefore each group in the Bank will review its internal control system on an on-going basis to keep it current and effective.

Objectives of Internal Controls

The internal controls are designed to provide reasonable assurance regarding the achievement of bank's objectives and help the management to evaluate processes and manage risks.

Broad objectives of Internal Controls include:

a) To ensure efficiency and effectiveness of operations;
b) To ensure reliability, completeness and timeliness of financial and management information;
c) To ensure compliance with applicable laws, regulations, policies and procedures.

2. Scope

The internal control policy is applicable across the Bank.

Internal Control Framework

The Internal Control Policy is aligned with the SBP Guidelines on Internal Controls issued vide BSD Circular No. 07 dated May 27, 2004 and accordingly the Bank adopted Internal Control-Integrated Framework of the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is most widely used internal control framework in the financial sector. The framework uses the bottom-up approach for risk assessment, in which risks are identified through process mapping and controls identification via developing process-flow charts.

3. Components of Internal Control

The BOP internal control structure consists of following interrelated components.

- Control environment
- Risk assessment and management
- Control Activities

- Accounting, Information & Communication
- Self-Assessment & Monitoring

3.1. Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It reflects the overall attitude, awareness and actions of the board and management concerning the importance of control activities.It is the foundation of all other components of the internal control, providing discipline and structure. Control environment factors include;

- The integrity, ethics and competence of personnel,
- Organizational structure of the institution,
- Oversight by the Board and senior management,
- Management philosophy and operating style,
- The way management assigns responsibility, organizes and develops its personnel,
- Attention and direction provided by the Board and its committees.

Accordingly, in order for internal controls to be effective, an appropriate control environment shall demonstrate the following behaviors;

- Board and management promote high ethical & integrity standards and establish a culture that emphasizes and demonstrates to all levels of personnel the importance of internal controls.
- Board approves and periodically reviews overall business strategies & policies of the bank and ensures that these are implemented.
- Board monitors effectiveness of internal control system.
- An independent internal audit function that directly report to the Board Audit Committee (BAC), which periodically tests and assess compliance with internal control policies / procedures and reports the instances of non-compliance.
- External Auditors interact with the BAC and present the Management Letter to the Board directly.
- Board ensures that appropriate remedial actions have been taken when instances of non-compliance are reported and internal control system has been improved to avoid recurring errors/mistakes.
- Management information system provides adequate information to the Board and they have access to bank's records, if need arises.
- Management ensures to set up internal control system across the bank to cover key risks areas to meet the bank’s objectives. Key Risk Areas include those core activities, the breakdown of which may render the Bank unable to meet its obligations to customers, regulators and the shareholders.
- Delegation of authority should be performed whenever practical. However, delegation of powers should be in writing and based on the appropriate skills and experience of the employee.
- No single individual (regardless of rank, title, or function) will process a specific transaction from initiation to final authorization. This means that four eyes principle shall be strictly

followed for all transactions prior to its completion. In case any individual is singly authorized to perform an end to end transaction, the risk associated with such exception shall be covered under banker's insurance policy.

- All procedures in force should ensure that transactions are correctly processed, authorized, completed, and recorded to provide an acceptable audit trail. Procedures should also prevent accidental or intentional damage to processing systems and records.
- The hiring process should be strictly in compliance with the approved HR policies ensuring Know Your Employee (KYE) procedures which must include credentials verification on timely basis.
- Training needs are periodically assessed and extended to enhance the skill set of employees. Third party employee should not be allowed any duty in violation of regulatory guidelines on outsourcing.
- All information systems and activities should be strictly subject to Bank's approved IT Security Policy.
- Exercising internal controls is the responsibility of every individual employee of the bank and violation to set policies & procedures are subject to accountability.
- SBP Outsourcing guidelines must be ensured by all the departments and any exception must be brought to the knowledge of CCG and corrective action should be taken immediately.
- P&OEG/HR function shall ensure "Job Rotation" where applicable and possible on best effort basis as a part of "Control Environment".

3.2. Risk Assessment and Management

Risk assessment is the process that the Board and management use to identify and analyze risks which could keep the Bank from achieving planned objectives. The assessment should help determine what the risks are, how they should be managed and what controls are needed.

- The Bank shall identify risks to the achievement of its objectives across the entity and analyzes them as a basis for determining how these risks should be managed.
- The Bank shall consider the potential for fraud in assessing risks to the achievement of objectives.
- The Bank shall identify and assesses changes that could significantly impact the system of internal controls.
- The Bank shall specify objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

The bank faces variety of risks that must be recognized and continually assessed. From an internal control perspective, a risk assessment should identify and evaluate the internal and external factors that could adversely affect achievement of its performance, information and compliance objectives.

Internal factors include complexity, nature and size of operations, quality of personnel, employee turnover, objectives and goals etc. External factors include fluctuating economic conditions, changes in the industry, technological advances, degree of aggressiveness of the market and

competition faced by the market participants etc. The risk identification should be done across the full spectrum of the activities, addressing measurable and non-measurable aspects of risks.

The risk evaluation is done to determine which risks are controllable and which are not. For those risks that are controllable, it must be assessed whether to accept those risks or the extent to which these could be mitigated through control procedures. For those risks that cannot be controlled, the senior management may decide whether to accept these risks or to withdraw from or reduce the level of business activity concerned. Internal controls may need to be revised to appropriately address any new or previously uncontrolled risks with the changing circumstances and conditions.

The Bank shall develop a strategy for identification, quantification, aggregation, mitigation, monitoring and reporting of operational risk. The operational risk assessment, key risk indicators, operational risk tolerance limits (thresholds) and periodic monitoring would be done in line with the Risk Management Policy and Operational Risk Management Framework of the Bank.

3.3. Control Activities

Control Activities are the policies and procedures that help to ensure that Board and management directives are carried out. These activities help to ensure that the Board and management manage and control risks that could affect Bank operating performance.

The control activities are designed and implemented to address the risk identified through the 'Risk Assessment and Management' process. The control activities involve two steps;

- Establishment of control policies and procedures.
- Verification that the control policies and procedures are being complied with.

Control activities occur throughout the organization, at all levels and in every business/function. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties. Control activities are most effective when these are made an integral part of the daily activities of all relevant personnel. Further, the duties are appropriately segregated so that personnel are not assigned conflicting responsibilities. Segregation of duties should be built into the selection and development of control activities.

The management shall establish and maintain a system of adequate internal controls and procedures which cover all their functions in general and key risk areas in particular, for implementing strategies and policies as approved by the Board designed to provide reasonable assurance as to the integrity and reliability with respect to effectiveness of those controls and reports produced there from. All employees must ensure implementation of defined controls in discharge of their respective functions.

3.4. Accounting, Information & Communication

Information & Communication systems ensure that risk-taking activities are within policy guidelines and that the systems are adequately tested and reviewed.

Information and communication systems capture and impart pertinent information in a form and timeframe that enables the Board, management and employees to carry out their responsibilities.

- The Bank obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.
- The Bank internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of other components of internal control.
- The Bank communicates with external parties regarding matters affecting the functioning of other components of internal control.

Accounting systems are the methods and records that identify, assemble, analyse, classify, record, and report the transactions in accordance with prescribed formats and international best practices.

Information systems are the reports on operations, finance, and compliance-related activities. The system should cover the full range of activities in such a manner that information remains understandable and useful for audit trail. The access to information systems is to be allowed or restricted as appropriate.

Communication systems impart significant information throughout the bank so that all personnel understand their own role, correlation of their activities with others and their responsibility in the control system. Significant information is also imparted to external parties such as regulators, shareholders, and customers as per statutory and regulatory requirements.

For effective information and communication system, management will ensure following:

- On a periodic basis (at least yearly) a communication to all employees of a Group shall be taken out by the respective Group Head/ Head advising them of the importance of internal controls in the Bank and reminding them of their responsibilities in this regard.

- In addition to effecting a control assessment, business managers must foster an environment that encourages all personnel to come forward and seek help when risks and control problems are recognized. While having a risk or control problem is never a good situation, allowing it to exist and worsen before escalation to senior management and not seeking help to get issues resolved is a scenario that cannot be tolerated.

- All Group / functions shall report issues (including control weaknesses, compliance issues and ineffectively controlled risks) in a timely manner, identified within their respective groups during the process of review of their processes/ Manuals.

3.5. Self-Assessment and Monitoring

Self-assessment and monitoring is an integral part of the internal control system. The process includes;

- Board and senior management oversight of the internal control, control reviews, and audit findings.

- The Bank selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

- The Bank evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the Board, as appropriate.

- All group / departments should report issues (including control weaknesses, compliance issues and ineffectively controlled risks) in a timely manner, identified within their respective groups through any of the following sources:
  - SBP Inspections
  - External Auditors – Management Letter
  - Internal Audit
  - Risk Management Group
  - Compliance & Control Group Reviews (as applicable)
  - Self-Assessment

- The Internal Audit Function (IAF) shall evaluate, during its periodic internal audits, the adequacy and effectiveness of self-assessment testing activities.

3.6. Internal Control Principles

Internal Control principles includes following:

a) **Cover all activities:** Bank shall develop internal controls which have coverage over all functions, in general, and the key risk areas (KRA) in particular. Key Risk Areas include those core activities, the breakdown of which may render the bank unable to meet its obligations to its customers, regulators and the sponsors. Examples of key risk areas are Liquidity Risk, Interest Rate Risk, Foreign Exchange Risk, Credit Risk, Operational Risk, compliance risk, reputational risk, etc.

b) **Regular Feature:** Control activities shall be an integral part of the daily activities of bank in such a manner that it becomes ingrained in their on-going processes.

c) **Segregation of Duties:** Duties shall be divided so that no one person has complete control over a key function or activity.

d) **Authorization and Approval:** All transactions shall be authorized before recording and execution.
e) **Custodial and Security Arrangements:** Responsibility for custody of assets needs to be separated from the related record keeping.
f) **Review and Reconciliation:** Records shall be examined and reconciled regularly to determine that transactions are properly processed, approved and booked.
g) **Physical Controls:** Equipment, inventories, cash and other assets shall be secured physically, counted periodically and compared with amounts shown on control records.
h) **Training and Supervision:** Qualified, well-trained and supervised employees help to ensure that control processes function properly.
i) **Documentation:** Documented policies and procedures promote employee understanding of duties and help to ensure continuity during employee absences or turnover. Therefore, policies and procedures shall exist in the Bank.
j) **Communication of Internal Controls:** Approved policies and procedures shall be accessible to relevant staff for reference and implementation.

Reporting of Internal Controls

A 'Statement on Internal Controls' shall be included in the annual report of the Bank. This statement should include following:

i. 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;
ii. Board of Directors' endorsement of the management's evaluation; and

In addition to above, the disclosure & reporting requirement regarding evaluation related to effectiveness of ICFR and overall internal controls shall be governed by the regulatory requirements.

4. Limitations of Internal Controls

The internal control system, no matter how well designed and operated, can only provide reasonable assurance to management and the Board of Directors regarding achievement of entity's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the realities that human judgment in decision-making can be faulty, and that breakdowns can occur because of such human failures as simple error or mistake. Moreover, controls can be avoided by the involvement of two or more persons, and management has the ability to override the internal control system. Another limiting factor is that even an effective internal control system can also experience a failure.