162 INTERNAL CONTROL FRAMEWORK

Internal control is a process designated and effected by the board of directors, senior management, and all levels of personnel to provide reasonable assurance on the achievement of objectives through efficient and effective operations; reliable, complete and timely financial and management information; and compliance with applicable laws, regulations, supervisory requirements, and the organization's policies and procedures.

Banks shall have in place adequate and effective internal control framework for the conduct of their business taking into account their size, risk profile and complexity of operations. The internal control framework shall embody management oversight and control culture; risk recognition and assessment; control activities; information and communication; and monitoring activities and correcting deficiencies.

Management oversight and control culture. Consistent with the principles provided under Secs. 132 (*Specific duties and responsibilities of the board of directors*) and 134 (*Duties and responsibilities of officers*), the board of directors and senior management shall be responsible for promoting high ethical and integrity standards; establishing the appropriate culture that emphasizes, demonstrates and promotes the importance of internal control; and designing and implementing processes for the prevention and detection of fraud.

a. The board of directors shall be ultimately responsible for ensuring that senior management establishes and maintains an adequate, effective and efficient internal control framework commensurate with the size, risk profile and complexity of operations of the bank. The board of directors shall also ensure that the internal audit function has an appropriate stature and authority within the bank and is provided with adequate resources to enable it to effectively carry out its assignments with objectivity.

    Further, the board of directors shall, on a periodic basis:

(1) conduct discussions with management on the effectiveness of the internal control system;

(2) review evaluations made by the audit committee on the assessment of effectiveness of internal control made by management, internal auditors and external auditors;

(3) ensure that management has promptly followed up on recommendations and concerns expressed by auditors and supervisory authorities on internal control weaknesses; and

(4) review and approve the remuneration of the head and personnel of the internal audit function. Said remuneration shall be in accordance with the bank's remuneration policies and

practices and shall be structured in such a way that these do not create conflicts of interest or compromise independence and objectivity.

The board of directors of UBs/KBs shall likewise commission an assessment team outside of the organization to conduct an independent quality assurance review of the internal audit function at least every five (5) years.

b. The audit committee shall be responsible for overseeing senior management in establishing and maintaining an adequate, effective and efficient internal control framework. It shall ensure that systems and processes are designed to provide assurance in areas including reporting, monitoring compliance with laws, regulations and internal policies, efficiency and effectiveness of operations, and safeguarding of assets.

The audit committee shall oversee the internal audit function and shall be responsible for:

(1) monitoring and reviewing the effectiveness of the internal audit function;

(2) approving the internal audit plan, scope and budget;

(3) reviewing the internal audit reports and the corresponding recommendations to address the weaknesses noted, discussing the same with the head of the internal audit function and reporting significant matters to the board of directors;

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

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

(6) reporting to the board of directors the annual performance appraisal of the head of the internal audit function;

(7) recommending for approval of the board of directors the annual remuneration of the head of the internal audit function and key internal auditors;

(8) appointing, reappointing or removing the head of the internal audit function and key internal auditors; and

(9) selecting and overseeing the performance of the internal audit service provider.

In particular, the audit committee shall be responsible for:

(1) ensuring independence of the internal audit service provider;

(2) reporting to the board of directors on the status of accomplishments of the outsourced internal audit activities, including significant findings noted during the conduct of the internal audit;

(3) ensuring that the internal audit service provider comply with sound internal auditing standards such as the Institute of Internal Auditors' International Standard for the Professional Practice of Internal Auditing and other supplemental standards issued by regulatory authorities/government agencies, as well as with relevant code of ethics;

(4) ensuring that the audit plan is aligned with the overall plan strategy and budget of the bank and is based on robust risk assessment; and

(5) ensuring that the internal audit service provider has adequate human resources with sufficient qualifications and skills necessary to accomplish the internal audit activities.

c. Senior management shall be responsible for maintaining, monitoring and evaluating the adequacy and effectiveness of the internal control system on an ongoing basis, and for reporting on the effectiveness of internal controls on a periodic basis. Management shall develop a process that identifies, measures, monitors and controls risks that are inherent to the operations of the bank; maintain an organizational structure that clearly assigns responsibility, authority and reporting relationships; ensure that delegated responsibilities are effectively carried out; implement internal control policies and ensure that activities are conducted by qualified personnel with the necessary experience and competence. Management shall ensure that bank personnel undertake continuing professional development and that there is an appropriate balance in the skills and resources of the front office, back office, and control functions. Moreover, management shall promptly inform the internal audit function of the significant changes in the bank's risk management systems, policies and processes.

d. All personnel need to understand their roles and responsibilities in the internal control process. They should be fully accountable in carrying out their responsibilities effectively and they should communicate to the appropriate level of management any problem in operations, action or behavior that is inconsistent with documented internal control processes and code of ethics.

Risk recognition and assessment. An effective internal control system shall identify, evaluate and continually assess all material risks that could affect the achievement of the bank's performance,

information and compliance objectives. The potential for fraud shall be considered in assessing the risks to the achievement of said objectives. Further, the risk assessment shall cover all risks facing the bank, which include, among others, credit; country and transfer; market; interest rate; liquidity; operational; compliance; legal; and reputational risks.

Effective risk assessment identifies and considers both internal (e.g., complexity of the organization's structure, nature of the bank's activities and personnel profile) and external (e.g., economic conditions, technological developments and changes in the industry) factors that could affect the internal control framework. The risk assessment shall be conducted at the level of individual business units and across all bank activities/groups/units and subsidiaries, in the case of a parent bank. Internal controls shall be revised to address any new or previously uncontrolled or unidentified risks.

Control activities. Control activities shall form part of the daily activities of the bank and all levels of personnel in the bank. Control activities are designed and implemented to address the risks identified in the risk assessment process. These involve the establishment of control policies and procedures, and verification that these are being complied with.

Banks shall have in place control activities defined at every business level, which shall include a system that provides for top and functional level reviews; checking compliance with exposure limits and follow-up on non-compliance; a system of approvals and authorizations, which shall include the approval process for new products and services; and a system of verification and reconciliation.

Control activities complement existing policies, procedures and other control systems in place such as, among others, having clearly defined organizational structure and reporting lines, and arrangements for delegating authority; adequate accounting policies, records and processes; robust physical and environmental controls for tangible assets and access controls to information assets; and appropriate segregation of conflicting functions.

a. *Clear arrangements for delegating authority.* The functions and scope of authority and responsibility of each personnel should be adequately defined, documented and clearly communicated. The extent to which authorities may be delegated and the corresponding accountabilities of the personnel involved shall be approved by the appropriate level of management or the board of directors.

b. *Adequate accounting policies, records and processes.* Banks shall maintain adequate financial policies, records and processes. These records shall be kept up-to-date and contain sufficient detail to establish an audit trail. Further, banks shall conduct independent balancing and reconciliation of records and reports to ensure the integrity of the reported data and balances. Banks shall also put in place a reliable information system that covers all of its significant

activities which shall allow the board of directors and management access to data and information relevant to decision making such as, among others, financial, operations, risk management, compliance and market information. Moreover, these systems shall be secured, monitored independently and supported by adequate contingency arrangements.

c. *Robust physical and environmental controls to tangible assets and access controls to information assets*. Banks shall adopt policies and practices to safeguard its tangible and information assets. These shall include, but shall not be limited to:

(1) identifying officers with authorities to sign for and on behalf of the bank. Signing authorities shall be approved by the board of directors and the extent of authority at each level shall be clearly defined;

(2) implementing joint custody on certain assets. Joint custody shall mean the processing of transactions in the presence, and under the direct observation, of a second person. Both persons shall be equally accountable for the physical protection of the items and records involved: Provided, That persons who are related to each other within the third degree of consanguinity or affinity shall not be made joint custodians;

(3) adopting dual control wherein the work of one (1) person is to be verified by a second person to ensure that the transaction is properly authorized, recorded and settled;

(4) incorporating sequence number control in the accounting system which shall also be used in promissory notes, checks and other similar instruments. Management shall also put in place appropriate controls to monitor the usage, safekeeping and recording of accountable forms;

(5) restricting access to information assets by classifying information as to degree of sensitivity and criticality and identifying information owners or personnel with authority to access particular classifications based on job responsibilities and the necessity to fulfill one’s duties; and

(6) implementing authentication and access controls prior to granting access to information such as, among others, implementing password rules. This shall be supplemented by appropriate monitoring mechanisms that will allow audit of use of information assets.

d. *Segregation of conflicting functions.* Banks shall ensure that areas of potential conflicts of interest shall be identified, minimized and subjected to independent monitoring. Further, appropriate segregation of functions shall be observed in identified areas that may pose potential conflict of interest. Moreover, periodic reviews of responsibilities and functions shall be conducted to

ensure that personnel are not in a position to conceal inappropriate actions.

Examples of internal control measures are in *Appendix 117*.

Information and communication. An effective internal control system requires that there are adequate and comprehensive internal financial, operational and compliance data, as well as external information about events and conditions that are relevant to decision making. Information shall be reliable, timely, accessible, and provided in a consistent format. Banks shall have in place a reliable management information system that covers significant activities of the bank and has the capability to generate relevant and quality information to support the functioning of internal control.

Banks shall also establish effective channels of communication to ensure that all personnel fully understand and adhere to policies and procedures and control measures relevant to their duties and responsibilities and that relevant information is reaching the appropriate personnel. Management shall also ensure that all personnel are cognizant of their duty to promptly report any deficiency to appropriate levels of management or to the board of directors, where required. These shall enable them to quickly respond to changing conditions and avoid unnecessary costs.

Monitoring activities and correcting deficiencies. The overall effectiveness of the internal controls shall be monitored on an ongoing basis. Monitoring functions and activities shall be adequately defined by management, integrated in the operating environment and should produce regular reports for review. In this regard, all levels of review shall be adequately documented and results thereof reported on a timely basis to the appropriate level of management.

Evaluations of the effectiveness of the internal control system and the corresponding monitoring activities may be done by personnel from the same operational area in the form of self-assessment or from other areas such as internal audit: *Provided*, That, self-assessment done by business units shall be subject to independent validation.

Evaluations done shall be adequately documented and internal control deficiencies and weaknesses identified shall be reported on a timely basis to the appropriate level of management or the board of directors, where necessary, and addressed promptly.

(Circular Nos. 969 dated 22 August 2017 and 871 dated 05 March 2015)