ANNEX 1

GUIDELINES FOR

INTERNAL CONTROL SYSTEMS IN BANKS

Date: 2 January 2018

CONTENTS

I. MANAGEMENT OVERSIGHT AND THE CONTROL CULTURE

A. THE BOARD OF DIRECTORS

Principle:

1. The board of directors is ultimately responsible for ensuring that an adequate and effective system of internal controls is established and maintained.

Guidelines:

1.1 A strong, active board, particularly when coupled with effective upward communication channels and capable financial, legal, and internal audit functions, provides an important mechanism to ensure the correction of problems that may diminish the effectiveness of the internal control system.

1.2 The board of directors must include in its activities:

(a) periodic discussions with management concerning the effectiveness of the internal control system;

(b) a timely review of evaluations of internal controls made by management, internal auditors, and external auditors;

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

(d) a periodic review of the appropriateness of the bank's strategy and risk limits.

1.3 Banks must follow the principles and guidance in the Guidelines for the Internal Audit Functions in Banks and the Guidelines for the Compliance and the Compliance Functions in Banks issued by the AMBD to assist the board in carrying out its internal control responsibilities.

1.4 A branch of a foreign bank licensed as a bank in Brunei Darussalam (Brunei branch of a foreign bank) must provide the AMBD with a satisfactory explanation how the bank's board of directors and senior management formalize and discharge their respective oversight responsibilities in relation to the Brunei branch of the foreign bank. This includes their responsibilities in terms of these Guidelines.

B. SENIOR MANAGEMENT

Principle:

2. Senior management must have responsibility for 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.

Guidelines:

2.1 Senior management is responsible for carrying out the directives of the board of directors, including the establishment of an effective system of internal control. Members of senior management must delegate responsibility for establishing more specific internal control policies and procedures to those responsible for a particular business unit. Delegation is an essential part of management; however, it is important to ensure that all delegations shall be within Board's framework/appetite. It is also important for senior management to oversee the managers to whom they have delegated these responsibilities to ensure that they develop and enforce appropriate policies and procedures.

2.2 Compliance with an established internal control system is heavily dependent on a well - documented and communicated organisational structure that clearly shows lines of reporting responsibility and authority and provides for effective communication throughout the organisation. The allocation of duties and responsibilities must ensure that there are no gaps in reporting lines and that an effective level of management control is extended to all levels of the bank and its various activities.

2.3 It is important that senior management takes steps to ensure that activities are conducted by qualified staff with the necessary experience and technical capabilities. Staff in control functions must be properly remunerated without causing conflicts of interest or inappropriate incentives which may interfere with their objectivity. Staff training and skills must be regularly updated. Senior management must institute compensation and promotion policies that reward appropriate behaviours and minimise incentives for staff to ignore or override internal control mechanisms.

C. CONTROL CULTURE

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 bank that emphasises and demonstrates to all levels of personnel the importance of internal controls. All personnel at a bank need to understand their role in the internal controls process and be fully engaged in the process.

Guidelines:

3.1 An essential element of an effective system of internal control is a strong control culture. It is the responsibility of the board of directors and senior management to emphasise the importance of internal control through their actions and words. This includes the ethical values that management displays in their business dealings, both inside and outside the organisation. The words, attitudes and actions of the board of directors and senior management affect the integrity, ethics and other aspects of the bank's control culture.

3.2 In varying degrees, internal control is the responsibility of everyone in a bank. Almost all employees produce information used in the internal control system or take other actions needed to effect control. An essential element of a strong internal control system is the recognition by all employees of the need to carry out their responsibilities effectively and to communicate to the appropriate level of management any problems in operations, instances of non-compliance with the bank's internal code of conduct, or other policy violations or illegal actions that are noticed. This can best be achieved when operational procedures are contained in clearly written documentation that is made available to all relevant personnel. It is essential that all personnel within the bank understand the importance of internal control and are actively engaged in the process.

3.3 In reinforcing ethical values, banks must avoid policies and practices that may inadvertently provide incentives or temptations for inappropriate activities. Examples of such policies and practices include undue emphasis on performance targets or other operational results, particularly short-term ones that ignore longer-term risks; compensation schemes that overly depend on short-term performance; ineffective segregation of duties or other controls that could allow the misuse of resources or concealment of poor performance; and insignificant or overly onerous penalties for improper behaviours.

3.4 While having a strong internal control culture does not guarantee that a bank will reach its goals, the lack of such a culture provides greater opportunities for errors to go undetected or for improprieties to occur.

II. RISK RECOGNITION AND ASSESSMENT

A. INCLUSION OF ALL ACTIVITIES

Principle:

4. An effective internal control system requires that the material risks which could adversely affect the achievement of the bank's goals are being recognised and continually assessed. This assessment must cover all risks facing the bank and the consolidated group (for example, 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.

Guidelines:

4.1 Banks are in the business of risk-taking. Consequently, it is imperative that, as part of an internal control system, these risks are being recognised and continually assessed. From an internal control perspective, a risk assessment must identify and evaluate the internal and external factors that could adversely affect the achievement of the bank's performance, information and compliance objectives. This process must cover all risks faced by the bank and operate at all levels within the bank. It differs from the risk management process which typically focuses more on the review of business strategies developed to maximise the risk/reward trade-off within the different areas of the bank.

4.2 Effective risk assessment identifies and considers internal factors (such as the complexity of the group structure, the nature of the bank's activities, the quality of personnel, organisational changes and employee turnover) as well as external factors (such as fluctuating economic conditions, changes in the industry and technological advances) that could adversely affect the achievement of the bank's goals. This risk assessment must be conducted at the level of individual businesses and across the wide spectrum of activities and subsidiaries of the consolidated bank group. This can be accomplished through various methods. Effective risk assessment addresses both measurable and non-measurable aspects of risks and weighs costs of controls against the benefits they provide.

4.3 The risk assessment process also includes evaluating the risks to determine which 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 whether to accept these risks or to withdraw from or reduce the level of business activity concerned.

4.4 In order for risk assessment, and therefore the system of internal control, to remain effective, senior management needs to continually evaluate the risks affecting the achievement of its goals and react to changing circumstances and conditions. Internal controls may need to be revised to appropriately address any new or previously uncontrolled risks. For example, as financial innovation occurs, a bank needs to evaluate new financial instruments and market transactions and consider the risks associated with these activities. Often these risks can be best understood when considering how various scenarios (economic and otherwise) affect the cash flows and earnings of financial instruments and transactions. Thoughtful consideration of the full range of possible problems, from customer misunderstanding to operational failure, will point to important control considerations.

III. CONTROL ACTIVITIES AND SEGREGATION OF DUTIES

A. CONTROLS TO BE 'TOP TO BOTTOM' AND WIDE RANGING

Principle:

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

Guidelines:

5.1 Control activities are designed and implemented to address the risks that the bank has identified through the risk assessment process described in Principle 4 above. Control activities involve two steps: (1) the establishment of control policies and procedures; and (2) verification that the control policies and procedures are being complied with. Control activities involve all levels of personnel in the bank, including senior management as well as front line personnel. Examples of control activities include:

(a) *Top level reviews* - Boards of directors and senior management often request presentations and performance reports that enable them to review the bank's progress toward its goals. For example, senior management may review reports showing actual financial results to date versus the budget. Questions that senior management generates as a result of this review and the ensuing responses of lower levels of management represent a control activity which may detect problems such as control weaknesses, errors in financial reporting or fraudulent activities.

(b) *Activity controls* - Department or division level management receives and reviews standard performance and exception reports on a daily, weekly or monthly basis. Functional reviews occur more frequently than top-level reviews and usually are more detailed. For instance, a manager of commercial lending may review weekly reports on delinquencies, payments received, and interest income earned on the portfolio, while the senior credit officer may review similar reports on a monthly basis and in a more summarised form that includes all lending areas. As with the top-level review, the questions that are generated as a result of reviewing the reports and the responses to those questions represent the control activity.

(c) *Physical controls* **-** Physical controls generally focus on restricting access to tangible assets, including cash and securities. Control activities include physical limitations, dual custody, and periodic inventories.

(d) *Compliance with exposure limits* - The establishment of prudent limits on risk exposures is an important aspect of risk management. For example, compliance with limits for borrowers and other counterparties reduces the bank's concentration of credit risk and helps to diversify its risk profile. Consequently, an important aspect of internal controls is a process for reviewing compliance with such limits and follow-up on instances of non-compliance.

(e) *Approvals and authorisations* - Requiring approval and authorisation for transactions over certain limits ensures that an appropriate level of management is aware of the transaction or situation, and helps to establish accountability.

(f) *Verifications and reconciliations* - Verifications of transaction details and activities and the output of risk management models used by the bank are important control activities. Periodic reconciliations, such as those comparing cash flows to account records and statements, may identify activities and records that need correction. Consequently, the results of these verifications must be reported to the appropriate levels of management whenever problems or potential problems are detected.

5.2 Control activities are most effective when they are viewed by management and all other personnel as an integral part of, rather than an addition to, the daily activities of the bank. When controls are viewed as an addition to the day-to-day activities, they are often seen as less important and may not be performed in situations where individuals feel pressured to complete activities in a limited amount of time. In addition, controls that are an integral part of the daily activities enable quick responses to changing conditions and avoid unnecessary costs. As part of fostering the appropriate control culture within the bank, senior management must ensure that adequate control activities are an integral part of the daily functions of all relevant personnel.

5.3 It is not sufficient for senior management to simply establish appropriate policies and procedures for the various activities and divisions of the bank. They must regularly ensure that all areas of the bank are in compliance with such policies and procedures and also determine that existing policies and procedures remain adequate. Where appropriate, in conducting an audit, the internal audit function will review the adequacy and effectiveness of the relevant policies and procedures.

B. SEGREGATION OF DUTIES AND AVOIDANCE OF CONFLICTS OF INTEREST

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 must be identified, minimised, and subject to careful, independent monitoring.

Guidelines:

6.1 One of the major causes of significant banking losses caused by poor internal controls is the lack of adequate segregation of duties. Assigning conflicting duties to one individual (for example, responsibility for both the front and back offices of a trading function) gives that person access to assets of value and the ability to manipulate financial data for personal gain or to conceal losses. Consequently, certain duties within a bank must be split, to the extent possible, among various individuals in order to reduce the risk of manipulation of financial data or misappropriation of assets.

6.2 Segregation of duties is not limited to situations involving simultaneous front and back office control by one individual. It can also result in serious problems when there are not appropriate controls in those instances where an individual has responsibility for:

(a) approval of the disbursement of funds and the actual disbursement;

(b) customer and proprietary accounts;

(c) transactions in both the "banking" and "trading" books;

(d) informally providing information to customers about their positions while marketing to the same customers;

(e) assessing the adequacy of loan documentation and monitoring the borrower after loan origination; and

(f) any other areas where significant conflicts of interest emerge and are not mitigated by other factors.

6.3 Areas of potential conflict must be identified, minimised, and subject to careful monitoring by an independent third party. There must also be periodic reviews of the responsibilities and functions of key individuals to ensure that they are not in a position to conceal inappropriate actions.

IV. INFORMATION AND COMMUNICATION

A. INFORMATION QUALITY

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 must be reliable, timely, accessible, and provided in a consistent format.

Guidelines:

7.1 Adequate information and effective communication are essential to the proper functioning of a system of internal control. From the bank's perspective, in order for information to be useful, it must be relevant, reliable, timely, accessible, and provided in a consistent format. Information includes internal financial, operational and compliance data, as well as external market information about events and conditions that are relevant to decision making. Internal information is part of a record-keeping process that must include established procedures for record retention.

B. ROBUST AND SECURE INFORMATION

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.

Guidelines:

8.1 A critical component of a bank's activities is the establishment and maintenance of management information systems that cover the full range of its activities. This information is usually provided through both electronic and non-electronic means. Banks must be particularly aware of the organisational and internal control requirements related to processing information in an electronic form and the necessity to have an adequate audit trail. Management decision-making could be adversely affected by unreliable or misleading information provided by systems that are poorly designed and controlled.

8.2 Electronic information systems and the use of information technology have risks that must be effectively controlled by banks in order to avoid disruptions to business and potential losses. Since transaction processing and business applications have expanded beyond the use of mainframe computer environments to distributed systems for mission critical business functions, the magnitude of risks also has expanded. Controls over information systems and technology must include both (a) general and (b) application controls.

(a) General controls are controls over computer systems (for example, mainframe, client/server, and end-user workstations) and ensure their continued, proper operation. General controls include in-house back-up and recovery procedures, software development and acquisition policies, maintenance (change control) procedures, and physical/logical access security controls.

(b) Application controls are computerised steps within software applications and other manual procedures that control the processing of transactions and business activities. Application controls include, for example, edit checks and specific logical access controls unique to a business system. Without adequate controls over information systems and technology, including systems that are under development, banks could experience loss of data and programs due to inadequate physical and electronic security arrangements, equipment or systems failures, and inadequate in-house backup and recovery procedures.

8.3 In addition to the risks and controls above, inherent risks exist that are associated with the loss or extended disruption of services caused by factors beyond the bank's control. In extreme cases, since the delivery of corporate and customer services represent key transactional, strategic and reputational issues, such problems could cause serious difficulties for banks and even jeopardise their ability to conduct key business activities. This possibility requires the bank to establish business resumption and contingency plans using an alternate off-site facility, including the recovery of critical systems supported by an external service provider. The potential for loss or extended disruption of critical business operations requires an institution-wide effort on contingency planning, involving business management, and not focused on centralised computer operations. Business resumption plans must be periodically tested to ensure the plan's functionality in the event of an unexpected disaster.

C. EFFICIENT COMMUNICATION

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.

Guidelines:

9.1 Without effective communication, information is useless. Senior management of banks need to establish effective paths of communication in order to ensure that the necessary information is reaching the appropriate people. This information relates both to the operational policies and procedures of the bank as well as information regarding its actual operational performance.

9.2 The organisational structure of the bank must facilitate an adequate flow of information - upward, downward and across the organisation. A structure that facilitates this flow ensures that information flows upward so that the board of directors and senior management are aware of the business risks and the operating performance of the bank. Information flowing down through an organisation ensures that the bank's objectives, strategies, and expectations, as well as its established policies and procedures, are communicated to all levels of management and operations personnel. This communication is essential to achieve a unified effort by all bank employees to meet the bank's objectives. Finally, communication across the bank is necessary to ensure that information that one division or department knows can be shared with other affected divisions or departments.

V. MONITORING ACTIVITIES AND CORRECTING DEFICIENCIES

Principle:

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

Guidelines:

10.1 Since banking is a dynamic, rapidly evolving industry, banks must continually monitor and evaluate their internal control systems in the light of changing internal and external conditions, and must enhance these systems as necessary to maintain their effectiveness. In complex, multinational organisations, senior management must ensure that the monitoring function is properly defined and structured within the organisation.

10.2 Monitoring the effectiveness of internal controls can be performed by personnel from several different areas, including the business function itself, financial control or internal audit. For that reason, it is important that senior management makes clear which personnel are responsible for which monitoring functions. Monitoring must be part of the daily activities of the bank but also include separate periodic evaluations of the overall internal control process. The frequency of monitoring different activities of a bank must be determined by considering the risks involved and the frequency and nature of changes occurring in the operating environment.

10.3 Ongoing monitoring activities can offer the advantage of quickly detecting and correcting deficiencies in the system of internal control. Such monitoring is most effective when the system of internal control is integrated into the operating environment and produces regular reports for review. Examples of ongoing monitoring include the review and approval of journal entries, and management review and approval of exception reports.

10.4 In contrast, separate evaluations typically detect problems only after the fact; however, separate evaluations allow an organisation to take a fresh, comprehensive look at the effectiveness of the internal control system and specifically at the effectiveness of the monitoring activities. These evaluations can be done by personnel form several different areas, including the business function itself, financial control and internal audit. Separate evaluations of the internal control system often take the form of self-assessments when persons responsible for a particular function determine the effectiveness of controls for their activities. The documentation and the results of the evaluations are then reviewed by senior management. All levels of review must be adequately documented and reported on a timely basis to the appropriate level of management.

Principle:

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

Guidelines:

11.1 Internal control deficiencies, or ineffectively controlled risks, must be reported to the appropriate person(s) as soon as they are identified, with serious matters reported to senior management and the board of directors. Once reported, it is important that management corrects the deficiencies on a timely basis. The internal auditors must conduct follow-up reviews or other appropriate forms of monitoring, and immediately inform senior management or the board of any uncorrected deficiencies. In order to ensure that all deficiencies are addressed in a timely manner, senior management must be responsible for establishing a system to track internal control weaknesses and actions taken to rectify them.

11.2 The board of directors and senior management must periodically receive reports summarising all control issues that have been identified. Issues that appear to be immaterial when individual control processes are looked at in isolation, may well point to trends that could, when linked, become a significant control deficiency if not addressed in a timely manner.

- END -