911 RISK MANAGEMENT

All covered persons shall develop sound risk management policies and practices to ensure that risks associated with ML/TF such as reputational, operational, and compliance risks are identified, assessed, monitored, mitigated and controlled, as well as to ensure effective implementation of this Part, to the end that covered persons shall not be used as a vehicle to legitimize proceeds of unlawful activity or to facilitate or finance terrorism.

The four (4) areas of sound risk management practices are adequate and active board and senior management oversight, acceptable policies and procedures embodied in a money laundering and terrorist financing prevention compliance program, appropriate monitoring and Management Information System and comprehensive internal controls and audit.

Board and senior management oversight. Notwithstanding the provisions specifying the duties and responsibilities of the compliance office and internal audit, it shall be the ultimate responsibility of the board of directors to fully comply with the provisions of this Part, these rules, the AMLA, as amended, the TFPSA and their RIRR. It shall ensure that ML/TF risks are effectively managed and that this forms part of the covered person's enterprise risk management system.

Senior management shall oversee the day-to-day management of the covered person, ensure effective implementation of AML/CFT policies approved by the board and alignment of activities with the strategic objectives, risk profile and corporate values set by the board. Senior management shall establish a management structure that promotes accountability and transparency and upholds checks and balances.

a. *Compliance office.* Management of the implementation of the covered person's Money Laundering and Terrorist Financing Prevention Program (MTPP) shall be a primary task of the compliance office. To ensure the independence of the office, it shall have a direct reporting line to the board of directors or any board-level or approved committee on all matters related to AML and TF compliance and their risk management. It shall be principally responsible for the following functions among other functions that may be delegated by senior management and the board, to wit:

(1) Ensure compliance by all responsible officers and employees with this Part, the AMLA, as amended, the RIRR and its own MTPP. It shall conduct periodic compliance checking which covers, among others, evaluation of existing processes, policies and procedures including on-going monitoring of performance by staff and officers involved in ML and TF prevention, reporting channels, effectiveness of the electronic money laundering transaction monitoring system and record retention system through sample testing and review of audit or

examination reports. It shall also report compliance findings to the board or any board-level committee;

(2) Ensure that infractions, discovered either by internally initiated audits, or by special or regular examiation conducted by the Bangko Sentral, or other applicable regulators, are immediately corrected;

(3) Inform all responsible officers and employees of all resolutions, circulars and other issuances by the Bangko Sentral and the AMLC in relation to matters aimed at preventing ML and TF;

(4) Alert senior management, the board of directors, or the board-level or approved committee if it believes that the covered person is failing to appropriately address AML/CFT issues; and

(5) Organize the timing and content of AML training of officers and employees including regular refresher trainings as stated in Sec. 932.

b. *Group-wide Money Laundering and Terrorist Financing Prevention Program (MTPP).* Financial groups shall implement group-wide MTPP, which shall be applied to their branches and majority-owned subsidiaries as provided in Sec. 903. The group-wide MTPP shall include the measures set out in this Section.

The group-wide compliance officer or in its absence, the compliance officer of the parent entity, shall oversee the AML/CFT compliance of the entire group with reasonable authority over the compliance officers of said branches, subsidiaries or offices.

Money Laundering and Terrorist Financing Prevention Program (MTPP). All covered persons shall adopt a comprehensive and risk-based MTPP geared toward the promotion of high ethical and professional standards and prevention of the covered person from being used, intentionally or unintentionally, for ML/TF activities. The MTPP shall include policies, controls and procedures to enable the covered persons to manage and mitigate the risks that have been identified in their risk assessment, including taking enhanced measures for those classified as posing higher risks. The MTPP shall also be consistent with the AMLA, as amended, the TFPSA, their respective RIRR and the provisions set out in this Part and designed according to the covered person’s corporate structure and risk profile. It shall be in writing, approved by the board of directors or by the country/regional head or its equivalent for local branches of foreign banks, and well disseminated to all officers and staff who are obligated by law and by their program to implement the same. Where a covered person has branches, subsidiaries, affiliates or offices located within and/or outside the Philippines, there shall be a consolidated ML/TF risk management system to ensure the coordination and implementation of policies and procedures on a group-wide basis, taking into account local business considerations, the

requirements of the host jurisdiction and the level of country risk.

The MTPP shall also be readily available in user-friendly form, whether in hard or soft copy. The covered person must put up a procedure to ensure an audit trail evidencing dissemination process for new and amended policies and procedures. The program shall embody the following at a minimum.

a. Detailed procedures of the covered person's compliance and implementation of the following major requirements of the AMLA, as amended, its RIRR, and this Part, to wit:

(1) Customer identification process including acceptance policies and on-going monitoring processes;

(2) Record keeping and retention;

(3) Covered transaction reporting; and

(4) ST reporting including the adoption of a system, electronic or manual, of flagging, monitoring and reporting of transactions that qualify as suspicious transactions, regardless of amount or that will raise a *"red flag"* for purposes of conducting further verification or investigation, or transactions involving amounts below the threshold to facilitate the process of aggregating them for purposes of future reporting of such transactions to the AMLC when their aggregated amounts breach the threshold. The ST reporting shall include a reporting chain under which a ST will be processed and the designation of a board-level or approved committee who will ultimately decide whether or not the covered person should file a report to the AMLC. If the resources of the covered person do not permit the designation of a committee, it may designate the compliance officer to perform this function instead: *Provided,* That the board of directors is informed of his decision.

b. An effective and continuous AML/CFT training program for all directors, and responsible officers and employees, to enable them to fully comply with their obligations and responsibilities under this Part, the AMLA, as amended, its RIRR and their internal policies and procedures as embodied in the MTPP. The training program shall also include refresher trainings to remind these individuals of their obligations and responsibilities as well as update them of any changes in AML laws, rules and internal policies and procedures.

c. An adequate screening and recruitment process to ensure that only qualified personnel who have no criminal record/s are employed to assume sensitive banking functions;

d. An internal audit system in accordance with this Section;

e. An independent audit program with written scope of audit that will ensure the completeness and accuracy of the information and identification documents obtained from clients, the covered and suspicious transactions reports submitted to the AMLC, and the records retained in compliance with this Part as well as adequacy and effectiveness of the training program on the prevention of money laundering and terrorism financing;

f. A mechanism that ensures all deficiencies noted during the audit and/or Bangko Sentral regular or special examination or other applicable regulator's examination are immediately corrected and acted upon;

g. Cooperation with AMLC and Bangko Sentral;

h. Designation of an AML compliance officer, who shall at least be at senior officer level, as the lead implementor of the program within an adequately staffed compliance office. The AML compliance officer may also be the liaison between the covered person, the Bangko Sentral and the AMLC in matters relating to the covered person's AML/CFT compliance. Where resources of the covered person do not permit the hiring of an AML compliance officer, the compliance officer shall also assume the responsibility of the former; and

i. Policies and procedures for sharing information required for the purposes of customer due diligence (CDD) and risk management;

j. A provision that the group-level compliance, audit, and/or AML/CFT functions should be provided with customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. This should include information on analysis of transactions or activities which appear unusual, if such analysis was done. Similarly, branches and subsidiaries should receive such information from these group-level functions when relevant and appropriate to risk management. The MTPP may require a potential and/or existing customer to sign a waiver on the disclosure of information within the group;

k. Adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off;

l. A mechanism to comply with freeze, bank inquiry and asset preservation orders, and all directives of the AMLC; and

m. A mechanism to comply with the prohibitions from conducting transactions with designated persons and entities, as set out in the relevant United Nations Security Council Resolutions (UNSCRs) relating to the prevention and suppression of terrorism and terrorist financing and

financing of proliferation of weapons of mass destruction.

Submission of the revised and updated MTPP. Approval by the board of directors or country head. Within six (6) months from 05 April 2017, all covered persons shall prepare and have available for inspection an updated MTPP, approved by the board of directors, embodying the principles and provisions stated in this Part.

Henceforth, each MTPP shall be regularly updated at least once every two (2) years to incorporate changes in AML policies and procedures, latest trends in ML and TF typologies, and latest pertinent Bangko Sentral issuances. Any revision or update in the MTPP shall likewise be approved by board of directors or the country/regional head or its equivalent for local branches of foreign banks.

Monitoring and reporting tools. All covered persons shall adopt an AML/CFT monitoring system that is appropriate for their risk profile and business complexity and in accordance with this Part. The system should be capable of generating timely, accurate and complete reports to lessen the likelihood of any reputational and compliance risks, and to regularly apprise the board of directors and senior management on AML/CFT compliance.

a. Electronic monitoring and reporting *systems for AML/CFT*. UBs and KBs and such covered persons that are considered complex pursuant to Sec. 131 (*Definition of terms*) shall adopt an electronic AML system capable of monitoring risks associated with ML/TF as well as generating timely reports for the guidance and information of its board of directors and senior management, in addition to the functionalities mentioned in Sec. 923 (*Electronic monitoring systems for AML/CFT*).

b. Manual monitoring. Covered persons not required to adopt an AML/CFT electronic system must ensure that they have the means of complying with this Section

Internal audit. The internal audit function associated with money laundering and terrorist financing should be conducted by qualified personnel who are independent of the office being audited. It must have the support of the board of directors and senior management and have a direct reporting line to the board or a board-level audit committee.

The internal audit shall, in addition to those specified by this Part, be responsible for the periodic and independent evaluation of the risk management, degree of adherence to internal control mechanisms related to the customer identification process, such as the determination of the existence of customers and the completeness of the minimum information and/or documents establishing the true and full identity of, and the extent and standard of due diligence applied to, customers, CT and ST reporting and record keeping and retention, as well as the adequacy and effectiveness of other existing internal controls associated with money laundering and terrorist financing.

For covered persons with electronic AML/CFT transaction monitoring system, in addition to the above, the internal audit shall include determination of the efficiency of the system's functionalities as required by this Section and Sec. 923 (*Electronic monitoring systems for AML/CFT*).

The results of the internal audit shall be timely communicated to the board of directors and shall be open for scrutiny by Bangko Sentral examiners in the course of the regular or special examination without prejudice to the conduct of its own evaluation whenever necessary. Results of the audit shall likewise be promptly communicated to the Compliance Office for appropriate monitoring of corrective actions taken by the different business units concerned. The Compliance Office shall regularly submit reports to the board to inform them of management's action to address deficiencies noted in the audit.

Risk assessment. Consistent with risk-based approach, covered persons are required to identify, understand and assess their ML/TF risks, arising from customers, countries or geographic areas of operations and customers, products, services, transactions or delivery channels. The assessment methodology shall be appropriate to the nature of operations and complexity of the business of the covered person. The institutional risk assessment shall (a) consider all relevant risk factors, including the results of national and sectoral risk assessments; (b) adequately document results and findings; and (c) be updated periodically or as necessary. The institutional risk assessment shall be conducted, at least once every two (2) years, or as often as the Board or senior management may direct, depending on the level or risks identified in the previous risk assessment or other relevant AML/CFT developments that may have an impact on the covered person's operations.

Based on the risk assessment, the covered person shall take appropriate measures to manage and mitigate ML/TF risks and take enhanced measures on identified high risks areas, which should be incorporated in its MTPP. The risk assessment shall be made available to the Bangko Sentral during examination or in other circumstances deemed necessary as part of continuous supervision.

New products and business practices risk assessment. Covered persons are also required to identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Such risk assessment should be an integral part of product or service development process and should take place prior to the launch of the new products, business practices or the use of new or developing technologies. Covered persons should take appropriate measures to manage and mitigate the identified risks.

(Circular No. 1022 dated 26 November 2018 and 950 dated 15 March 2017)