Annex of Decree of the Governor of
the Bank of Mongolia, Dated February 6,2018

Bank of Mongolia

AML/CFT Risk Based Management Guidance Note

Introduction

The Bank of Mongolia (BOM) expects all institutions to develop effective frameworks and practices to manage their money laundering/terrorist financing risks (ML/TF). The effective management of risks is a requirement of the Financial Action Task Force (FATF) Recommendations. The FATF Recommendation 1 requires countries at a national level to identify, assess and understand country specific ML/TF risks. In addition, it is expected that countries will ensure that financial institutions identify and assess ML/TF risks arising from their operations and take the measures necessary to effectively mitigate such risks. This risk assessment and any underlying information should be documented, kept up-to-date and readily available for the BOM to review at its request.

The BOM recognizes that financial institutions are exposed to ML/TF risks which arise from the general economic environment in Mongolia and from the nature of their own operations. In accordance with the above-mentioned international standards and international best practices for risk management, the BOM expects institutions to develop a framework and practices to effectively identify, measure, monitor, control and mitigate ML/TF risks.

The Risk Management Process

- **Identification**

Identification is the first stage of the risk management process. The BOM expects institutions to be aware of the ML/TF risks that are implicit in their operations. These risks arise from a number of sources including customers, products and services, delivery channels and geographic regions and markets. Institutions must therefore be able to aware of and identify the types of ML/TF risks that arise from each of these sources.

Financial institutions should also be aware of the ML/TF risks that exist in Mongolia in general, including for example those identified in Mongolia's National Risk Assessment which is available on the Bank of Mongolia's website, www.mongolbank.mn. At a national level this process requires the identification of risk factors associated with ML/TF threats and vulnerabilities. Threats are a function of the general levels of criminal and terrorist activity to which a country is exposed. Vulnerabilities are a function of political, (the characteristics of the political system), economic, (the nature of economic activity) social, (demographic characteristics), technological (level of technological advancement), environmental (issues

related to the physical environment) and legislative (the coverage, maturity and effectiveness of the legislative system) factors.

- **Measuring**

The identification or recognition of risk is the first step in an effective risk management process. Beyond identifying risk, it is equally important to measure or quantify risk. Unless it is effectively measured it is difficult to assess the potential impact that a given type or source of risk can have on an institution. Institutions are therefore expected to develop techniques and mechanisms which will allow them to assess the quantum of each type of ML/TF risk with which it is faced and the likely duration of such risk. If, for example, an institution considers a specific type of customer to represent a high ML/TF risk, the BOM expects that the institution should at all times be aware of the number of such customers it has and the types and volume of business activity and transactions they are conducting.

- **Controlling**

Having identified and measured risks, the BOM expects institutions to develop a risk management framework and practices to effectively mitigate such risks. This requires the development of policies that reflect the institution's risk appetite and its approach to risk management, procedures that give effect to the policies and limits that preclude undesirable levels of risk concentrations or exposures. An important aspect of a framework for controlling risk is the establishment of clear lines of authority and reporting lines and responsibilities within institutions. Effective control of risk is also dependent on the institution's ability to communicate its policies, procedures and limits to all employees and business units involved in the management of ML/TF risks, and to apply the risk-control measures and resources commensurately with assessed risks.

- **Monitoring**

The BOM expects institutions to establish effective systems for the on-going monitoring of their risk exposures and the effectiveness of associated risk management systems and practices. Institutions are therefore expected to have Management Information Systems (MIS) that measure their inherent ML/TF risks and changes in such exposures. In the context of ML/TF risks it is important, for example, that the MIS monitors the increase or decrease of the institution's exposure to ML/TF risk. The MIS should also, for example, monitor customer behavior and transactions to identify activity that may arouse suspicion of being linked to ML/TF. Further, the MIS should monitor the adherence to established policies and procedures to determine, for example, when an established internal limit or legal and regulatory obligations have been breached.

- **Mitigation**

The successful mitigation of ML/TF risks is the outcome of all of the above measures if they are effectively and consistently implemented.

The Risk Management Framework

1. Corporate Governance

BOM expects financial institutions to establish a robust and effective corporate governance framework that ensures transparency, accountability and high ethical conduct in all aspects of their operations. Institutions should adopt a Code of Ethics that promotes consistently high standards of ethical conduct by all employees. A sound corporate governance framework includes the use of effective policies and procedures, monitoring and reporting mechanisms and internal controls. Measures that ensure appropriate separation of functions and the avoidance of conflicts of interests are essential hallmarks of an effective corporate governance regime. The Board of Directors (BOD) is ultimately responsible for establishing a corporate vision strategy and business model and for overseeing an institution's corporate governance culture and is expected to develop mechanisms including board committees to achieve this objective. Senior management is responsible for ensuring the effective functioning of the corporate governance framework on a day-to day basis.

- *Board of Directors*

  Members of the BOD should have a good understanding of the institution's business model and operations and the general business climate in which it operates. They should have the qualifications and experience necessary to understand the institution's business model and operations and how these relate to Mongolia's general economic and social environment. The BOD should ideally be comprised of both executive and non-executive directors to ensure a desirable level of independence from the institution's management function.

  The BOD should establish the institution's overall risks appetite and should ensure that mechanisms are in place to effectively mitigate risk. The BOD must ensure that appropriate policies, procedures and controls are in place to manage such risks and should also ensure that arrangements are in place for the effective reporting on all issues related to the functioning of the risk management framework. The BOD is ultimately responsible for the institution's operations, its management of the risk to which it is exposed and its compliance with all laws, regulations and guidelines to which it is subject.

- *Senior Management*

  An institution's senior management is responsible for implementing the corporate vision, strategy and business model approved by the BOD. Senior management should demonstrate a firm understanding of all aspects of the institution's business model and is responsible for developing the components of the risk management framework. Senior management is responsible for ensuring that the institution has all the resources necessary

to effectively manage risk. They are also responsible for ensuring that effective communication and reporting arrangements are in place to support good risk management practices. This includes ensuring that all staff members are aware of the requirements of the risk management framework and their specific roles and responsibilities.

Senior management is responsible for ensuring that internal reporting mechanisms, including reports to be sent to the BOD, are developed to provide accurate and timely information relevant to the effective management of risks.

- *The Risk Management Function*

The BOM expects institutions to develop an effective risk management function. The risk management function is the business unit with day to day operational responsibility for ensuring that the institution effectively identifies, measures, monitors, and controls and mitigates risks. From a day-to-day operational perspective risk management supports senior management and the BOD to achieve the ML/TF risk management objectives discussed in this guidance note. The risk management function should be commensurate with the, size, nature and complexity of the institution's business model and operations.

2. Policies and Procedures

The BOM expects the senior management to develop policies and procedures to effectively manage the ML/TF risks that arise from an institution's operations. Policies and procedures developed by senior management should be approved by the BOD. Policies and procedures should set out the day to day measures that should be employed to ensure that the institution effectively identifies, measures, monitors and controls ML/TF risks. They should therefore be developed to reflect the risks implicit in an institution's customers, products and services, delivery channels and geographic regions. Policies and procedures should be comprehensively documented and communicated to all staff. They should also be subject to periodic review to ensure they are appropriate in light of changes to the institution's ML/TF risk profile.

Policies and procedures should clearly set out lines of responsibility and accountability for the execution of the risk management function and should also establishing effective reporting lines for all persons and business units involved in the management of ML/TF risks.

An effective risk management framework should establish limits in the context of the institution's stated appetite for ML/TF risk and the overall effective implementation of the risk management system. Policies and procedures should limit, for example, an institution's exposure to the ML/TF risks arising from exposure to specific types of customers, products and services, delivery channels and geographic regions/markets. An effective ML/TF risk management framework should include a mechanism to report incidents where established limits have been breached and the frequency of such events.

3. Internal Controls

An on-going system of internal controls is an essential component of a risk management framework. Institutions are expected to employ measures on an on-going basis to ensure adherence to establishes policies and procedures as well as relevant laws, regulations and guidelines.

Arrangements should be in place to reinforce the four eyes principle and avoid conflicts of interest. Measures should be employed, for example, to ensure adequate separation between operational and control functions such as front office and back office activities.

Institutions are also expected to ensure that their ML/TF risk management framework and practices are subject to external audit review.

4. Internal audit

Institutions are expected to develop effective internal audit arrangements. The internal audit function should be an independent function with a direct reporting line to the Board Audit Committee. The internal audit function should periodically assess the effectiveness of the institutions' ML/FT risk management framework and practices paying specific attention to the institution's adherence to established policies procedures and limits and applicable laws, regulations and guidelines.

5. The Compliance Function

The BOM expects institutions to develop an effective compliance function as a component of its ML/TF risk management framework. The compliance function should be commensurate with the, size, nature and complexity of the institution's business model and operations. The compliance function is separate from the internal audit function as it is a component of an institutions day-to-day operational activity.

The compliance function should on an-ongoing basis assess the extent to which the institution is complying with established policies, procedures and limits and obligations arising from applicable laws, regulations and guidelines. The effectiveness of the compliance function rests heavily on the effectiveness with which the MIS generates accurate and timely reports related to the management of ML/TF risks.

6. Risk Monitoring and Reporting

To effectively control and mitigate risk institutions need to develop robust MIS systems that provide reliable data on the quantity and nature of ML/TF risks and the effectiveness with which risks are being mitigated. The MIS system used by an institution should be commensurate with the size, nature and complexity of its business model and operations. Such systems should constantly measure the quantity of ML/TF risks, changes to nature of such risks and should also report on adherence to the policies and procedures designed to

mitigate risks. The system should, for example, not only identify instances in which policies and procedures have been breached but should maintain a record of all such incidents.

The system should provide timely reports to all business units and senior management to allow them to make judgments on the measures necessary to manage risks. Reports should also be prepared and submitted to senior management and the BOD indicating how well the institution is managing risk and highlighting instances of breaches of risk management policies, procedures and limits and obligations arising from applicable laws, regulations and guidelines.

7. Training

The BOM expects institutions to have effective arrangements in place to train their staff on all issues related to their AML/CFT regime. It is important that staff understand the institution's inherent ML/TF risks and the nature of the measures that have been developed to mitigate these risks. Training must be provided for all staff on joining the institution and should be an-ongoing activity. Apart from general training provided to all staff, targeted training programs should be developed for specific categories of staff in light of the nature of their work in the context of ML/FT risks. AML/CFT awareness raising programs should be conducted for members of the Board of Directors.