Asia/Pacific Group on Money Laundering

APG THIRD ROUND MUTUAL EVALUATIONS

INDONESIA

CONTENT **Page**

Asia/Pacific Group
on Money Laundering

PART A:

QUESTIONNAIRE FOR TECHNICAL COMPLIANCE UPDATE

[2017/02/20]

Background and Key documents

Jurisdictions should briefly note any significant changes to their AML/CFT system which have taken place since the last evaluation or since they exited the follow-up process. This includes:

- New AML/CFT laws, regulations and enforceable means;
- New competent authorities, or significant reallocation of responsibility between competent authorities.

Jurisdictions should list the principal laws and regulations in their AML/CFT system, and give a brief, high-level summary of their scope. The (translated) text of these laws should be provided to assessors. It is preferable to assign each document a unique number to ensure references are consistent. These numbers should be listed here.

Jurisdictions should list the main competent authorities responsible for AML/CFT policy and operations, and summarise their specific AML/CFT responsibilities.

1. [Example –"Since the last evaluation, Jurisdiction X has passed the 'Law on Suspicious Transaction Reporting (2009)' and established an FIU. Responsibility for investigating suspicious transactions has been transferred from the Ministry of Interior to the FIU.

2. [Example –"The principal laws relevant to AML/CFT are:

- *Money Laundering Act (1963) (document L1) – establishes a criminal offence of money laundering*
- *Proceeds of Crime Act (2007) (document L2) – sets a legal framework for confiscation of the proceeds of crime*
- *National Security Act (2005) (document L3) – establishes a criminal offence of terrorist financing and a legal framework for implementing targeted financial sanctions*
- *Financial Sector Act (1999) (document L4) – provides the legal basis for financial sector regulation and supervision and sets out the basic AML/CFT obligations on firms. ...*

Risk and Context

Jurisdictions should provide assessors with available documents about the ML/TF risks in their jurisdiction. They should list each document they provide, and briefly describe their scope. Jurisdictions should also note any important considerations about risk and context which they wish to bring to the attention of assessors. This should not duplicate information included in the documents provided. If jurisdictions wish to highlight specific contextual factors, they should provide documentation on these.

Jurisdictions should describe the size and structure of their financial and DNFBP sectors, using the tables in Annex I.

Technical Compliance Information

Jurisdictions should provide information on their technical compliance with each of the Criteria used in the FATF Methodology.

For each criterion, jurisdictions should, as a minimum, set out the reference (name of instrument, article or section number) that applies. Jurisdictions should refer to the *specific clauses* of their laws, enforceable means, or other mechanisms which are relevant to the criterion. *If necessary* jurisdictions should also *briefly* explain the elements of their laws, enforceable means, or other mechanisms which implement the criterion, (e.g. an outline of the procedures followed, or an explanation of the interaction between two laws). Jurisdictions should also note whether the law or enforceable means referred to has changed since the last MER or follow-up report.

The (translated) text of all relevant laws, enforceable means, and other documents should be provided separately (but as early as possible).

Jurisdictions should provide brief factual information only – there is no need for lengthy argument or interpretation. There is no need to set out each criterion in full. Information could be provided in the following form:

Recommendation 1

1.1: Countries[1] should identify and assess the ML/TF risks for the country

1.2: Countries should designate an authority or mechanism to coordinate actions to assess risks

1.3: Countries should keep the risk assessments up-to-date

1.4: Countries should have mechanisms to provide information on the results of the risk assessment(s) to all relevant competent authorities and self-regulatory bodies (SRBs), financial institutions and DNFBPs

Risk mitigation

1.5 Based on their understanding of their risks, countries should apply a risk-based approach to allocating resources and implementing measures to prevent or mitigate ML/TF.

1.6 Countries which decide not to apply some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions, should demonstrate that:

(a) there is a proven low risk of ML/TF; the exemption occurs in strictly limited and justified circumstances; and it relates to a particular type of financial institution or activity, or DNFBP; or

(b) a financial activity (other than the transferring of money or value) is carried out by a natural or legal person on an occasional or very limited basis (having regard to quantitative and absolute criteria), such that there is a low risk of ML/TF.

1.7 Where countries identify higher risks, they should ensure that their AML/CFT regime addresses such risks, including through: (a) requiring financial institutions and DNFBPs to take enhanced measures to manage and mitigate the risks; or (b) requiring financial institutions and DNFBPs to ensure that this

[1] Where appropriate, ML/TF risk assessments at a supra-national level should be taken into account when considering whether this obligation is satisfied.

information is incorporated into their risk assessments.

1.8 Countries may allow simplified measures for some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions, provided that a lower risk has been identified, and this is consistent with the country's assessment of its ML/TF risks.

1.9 Supervisors and SRBs should ensure that financial institutions and DNFBPs are implementing their obligations under Recommendation 1.

Risk assessment

1.10 Financial institutions and DNFBPs should be required to take appropriate steps to identify, assess, and understand their ML/TF risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels). This includes being required to:

(a) document their risk assessments;

(b) consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied;

(c) keep these assessments up to date; and

(d) have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs.

Risk mitigation

1.11 Financial institutions and DNFBPs should be required to:

(a) have policies, controls and procedures, which are approved by senior management, to enable them to manage and mitigate the risks that have been identified (either by the country or by the financial institution or DNFBP);

(b) monitor the implementation of those controls and to enhance them if necessary; and

(c) take enhanced measures to manage and mitigate the risks where higher risks are identified.

1.12 Countries may only permit financial institutions and DNFBPs to take simplified measures to manage and mitigate risks, if lower risks have been identified, and criteria 1.9 to 1.11 are met. Simplified measures should not be permitted whenever there is a suspicion of ML/TF.

Recommendation 2 - National Cooperation and Coordination

2.1 Countries should have national AML/CFT policies which are informed by the risks identified, and are regularly reviewed.

2.2 Countries should designate an authority or have a coordination or other mechanism that is responsible for national AML/CFT policies.

2.3 Mechanisms should be in place to enable policy makers, the FIU, law enforcement authorities, supervisors and other relevant competent authorities to co-operate, and where appropriate, coordinate domestically with each other concerning the development and implementation of AML/CFT policies and activities. Such mechanisms should apply at both policymaking and operational levels.

2.4 Competent authorities should have similar co-operation and, where appropriate, co-ordination mechanisms to combat the financing of proliferation of weapons of mass destruction.

Recommendation 3 - Money Laundering Offence

3.1 ML should be criminalised on the basis of the Vienna Convention and the Palermo Convention (see Article 3(1)(b)&(c) Vienna Convention and Article 6(1) Palermo Convention).

3.2 The predicate offences for ML should cover all serious offences, with a view to including the widest range of predicate offences. At a minimum, predicate offences should include a range of offences in each of the designated categories of offences.

3.3 Where countries apply a threshold approach or a combined approach that includes a threshold approach, predicate offences should, at a minimum, comprise all offences that:

(a) fall within the category of serious offences under their national law; or

(b) are punishable by a maximum penalty of more than one year's imprisonment; or

(c) are punished by a minimum penalty of more than six months' imprisonment (for countries that have a minimum threshold for offences in their legal system).

3.4 The ML offence should extend to any type of property, regardless of its value, that directly or indirectly represents the proceeds of crime.

3.5 When proving that property is the proceeds of crime, it should not be necessary that a person be convicted of a predicate offence.

3.6 Predicate offences for money laundering should extend to conduct that occurred in another country, which constitutes an offence in that country, and which would have constituted a predicate offence had it occurred domestically.

3.6 The ML offence should apply to persons who commit the predicate offence, unless this is contrary to fundamental principles of domestic law.

3.8 It should be possible for the intent and knowledge required to prove the ML offence to be inferred from objective factual circumstances.

3.9 Proportionate and dissuasive criminal sanctions should apply to natural persons convicted of ML.

3.10 Criminal liability and sanctions, and, where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which more than one form of liability is available. Such measures are without prejudice to the criminal liability of natural persons. All sanctions should be proportionate and dissuasive.

3.11 Unless it is not permitted by fundamental principles of domestic law, there should be appropriate ancillary offences to the ML offence, including: participation in; association with or conspiracy to commit; attempt; aiding and abetting; facilitating; and counselling the commission.

Recommendation 4 - Confiscation and Provisional Measures

4.1 Countries should have measures, including legislative measures that enable the confiscation of the following, whether held by criminal defendants or by third parties:

(a) property laundered;

(b) proceeds of (including income or other benefits derived from such proceeds), or instrumentalities used or intended for use in, ML or predicate offences;

(c) property that is the proceeds of, or used in, or intended or allocated for use in the financing of terrorism, terrorist acts or terrorist organisations; or

(d) property of corresponding value.

4.2 Countries should have measures, including legislative measures, that enable their competent authorities to:

(a) identify, trace and evaluate property that is subject to confiscation;

(b) carry out provisional measures, such as freezing or seizing, to prevent any dealing, transfer or disposal of property subject to confiscation ;

(c) take steps that will prevent or void actions that prejudice the country's ability to freeze or seize or recover property that is subject to confiscation; and

(d) take any appropriate investigative measures.

4.3 Laws and other measures should provide protection for the rights of bona fide third parties.

4.4 Countries should have mechanisms for managing and, when necessary, disposing of property frozen, seized or confiscated.

Recommendation 5 – Terrorist Financing Offence

5.1 Countries should criminalise TF on the basis of the Terrorist Financing Convention.

5.2 TF offences should extend to any person who wilfully provides or collects funds by any means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they are to be used, in full or in part: (a) to carry out a terrorist act(s); or (b) by a terrorist organisation or by an individual terrorist (even in the absence of a link to a specific terrorist act or acts).

5.3 TF offences should extend to any funds whether from a legitimate or illegitimate source.

5.4 TF offences should not require that the funds: (a) were actually used to carry out or attempt a terrorist act(s); or (b) be linked to a specific terrorist act(s).

5.5 It should be possible for the intent and knowledge required to prove the offence to be inferred from objective factual circumstances.

5.6 Proportionate and dissuasive criminal sanctions should apply to natural persons convicted of TF.

5.7 Criminal liability and sanctions, and, where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which more than one form of liability is available. Such measures should be without prejudice to the criminal liability of natural persons. All sanctions should be proportionate and dissuasive.

5.8 It should also be an offence to:

(a) attempt to commit the TF offence;

.

(b) participate as an accomplice in a TF offence or attempted offence;

(c) organise or direct others to commit a TF offence or attempted offence; and

(d) contribute to the commission of one or more TF offence(s) or attempted offence(s), by a group of persons acting with a common purpose.

5.9 TF offences should be designated as ML predicate offences.

5.10 TF offences should apply, regardless of whether the person alleged to have committed the offence(s) is in the same country or a different country from the one in which the terrorist(s)/terrorist organisation(s) is located or the terrorist act(s) occurred/will occur.

Recommendation 6 – Targeted Financial Sanctions related to Terrorism and Terrorist Financing

Identifying and designating

6.1 In relation to designations pursuant to United Nations Security Council - 1267/1989 (Al Qaida) and 1988 sanctions regimes (Referred to below as "UN Sanctions Regimes"), countries should:

(a) identify a competent authority or a court as having responsibility for proposing persons or entities to the 1267/1989 Committee for designation; and for proposing persons or entities to the 1988 Committee for designation;

(b) have a mechanism(s) for identifying targets for designation, based on the designation criteria set out in the relevant United Nations Security Council resolutions (UNSCRs);

(c) apply an evidentiary standard of proof of "reasonable grounds" or "reasonable basis" when deciding whether or not to make a proposal for designation. Such proposals for designations should not be conditional upon the existence of a criminal proceeding;

(d) follow the procedures and (in the case of UN Sanctions Regimes) standard forms for listing, as adopted by the relevant committee (the 1267/1989 Committee or 1988 Committee); and

(e) provide as much relevant information as possible on the proposed name ; a statement of case which contains as much detail as possible on the basis for the listing ; and (in the case of proposing names to the 1267/1989 Committee), specify whether their status as a designating state may be made known.

6.2 In relation to designations pursuant to UNSCR 1373, countries should:

(a) identify a competent authority or a court as having responsibility for designating persons or entities that meet the specific criteria for

designation, as set forth in UNSCR 1373; as put forward either on the country's own motion or, after examining and giving effect to, if appropriate, the request of another country.

(b) have a mechanism(s) for identifying targets for designation, based on the designation criteria set out in resolution 1373 ;

(c) when receiving a request, make a prompt determination of whether they are satisfied, according to applicable (supra-) national principles that the request is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in UNSCR 1373;

(d) apply an evidentiary standard of proof of "reasonable grounds" or "reasonable basis" when deciding whether or not to make a designation . Such (proposals for) designations should not be conditional upon the existence of a criminal proceeding; and

(e) when requesting another country to give effect to the actions initiated under the freezing mechanisms, provide as much identifying information, and specific information supporting the designation, as possible.

6.3 The competent authority(ies) should have legal authorities and procedures or mechanisms to:

(a) collect or solicit information to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation; and

(b) operate ex parte against a person or entity who has been identified and whose (proposal for) designation is being considered.

Freezing

6.4 Countries should implement targeted financial sanctions without delay.

6.5 Countries should have the legal authority and identify domestic competent authorities responsible for implementing and enforcing targeted financial sanctions, in accordance with the following standards and procedures:

(a) Countries should require all natural and legal persons within the country to freeze, without delay and without prior notice, the funds or other assets of designated persons and entities.

(b) The obligation to freeze should extend to: (i) all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular terrorist act, plot or threat; (ii) those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and (iii) the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as (iv) funds or other assets of persons and entities acting on behalf of, or at the direction of, designated persons or entities.

(c) Countries should prohibit their nationals, or any persons and entities within their jurisdiction, from making any funds or other assets, economic resources, or financial or other related services, available, directly or indirectly, wholly or jointly, for the benefit of designated persons and entities; entities owned or controlled, directly or indirectly, by designated persons or entities; and persons and entities acting on behalf of, or at the direction of, designated persons or entities, unless licensed, authorised or otherwise notified in accordance with the relevant UNSCRs.

(d) Countries should have mechanisms for communicating designations to the financial sector and the DNFBPs immediately upon taking such action, and providing clear guidance to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms.

(e) Countries should require financial institutions and DNFBPs to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant UNSCRs, including attempted transactions.

(f) Countries should adopt measures which protect the rights of bona fide third parties acting in good faith when implementing the obligations under Recommendation 6.

De-listing, unfreezing and providing access to frozen funds or other assets

6.6 Countries should have publicly known procedures to de-list and unfreeze the funds or other assets of persons and entities which do not, or no longer, meet the criteria for designation. These should include:

(a) procedures to submit de-listing requests to the relevant UN sanctions Committee in the case of persons and entities designated pursuant to the UN Sanctions Regimes, in the view of the country, do not or no longer meet the criteria for designation. Such procedures and criteria should be in accordance with procedures adopted by the 1267/1989 Committee or the 1988 Committee, as appropriate;

(b) legal authorities and procedures or mechanisms to de-list and unfreeze the funds or other assets of persons and entities designated pursuant to UNSCR 1373, that no longer meet the criteria for designation;

(c) with regard to designations pursuant to UNSCR 1373, procedures to allow, upon request, review of the designation decision before a court or other independent competent authority;

(d) with regard to designations pursuant to UNSCR 1988, procedures to facilitate review by the 1988 Committee in accordance with any applicable guidelines or procedures adopted by the 1988 Committee, including those of the Focal Point mechanism established under UNSCR 1730;

(e) with respect to designations on the Al-Qaida Sanctions List, procedures for informing designated persons and entities of the availability of the United Nations Office of the Ombudsperson, pursuant to UNSCRs 1904, 1989, and 2083 to accept de-listing petitions.

(f) publicly known procedures to unfreeze the funds or other assets of persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by a freezing mechanism (i.e. a false positive), upon verification that the person or entity involved is not a designated person or entity; and

(g) mechanisms for communicating de-listings and unfreezings to the financial sector and the DNFBPs immediately upon taking such action, and

providing guidance to financial institutions and other persons or entities, including DNFBPs, that may by holding targeted funds or other assets, on their obligations to respect a de-listing or unfreezing action.

6.7 Countries should authorise access to frozen funds or other assets which have been determined to be necessary for basic expenses, for the payment of certain types of fees, expenses and service charges, or for extraordinary expenses, in accordance with the procedures set out in UNSCR 1452 and any successor resolutions. On the same grounds, countries should authorise access to funds or other assets, if freezing measures are applied to persons and entities designated by a (supra) national country pursuant to UNSCR 1373.

Recommendation 7 – Target Financial Sanctions related to Proliferation

7.1 Countries should implement targeted financial sanctions without delay to comply with United Nations Security Council resolutions, adopted under Chapter VII of the Charter of the United Nations, relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing.

7.2 Countries should establish the necessary legal authority and identify competent authorities responsible for implementing and enforcing targeted financial sanctions, and should do so in accordance with the following standards and procedures.

(a) Countries should require all natural and legal persons within the country to freeze, without delay and without prior notice, the funds or other assets of designated persons and entities.

(b) The freezing obligation should extend to: (i) all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular act, plot or threat of proliferation; (ii) those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and (iii) the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as (iv) funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities.

(c) Countries should ensure that any funds or other assets are prevented from being made available by their nationals or by any persons or entities within their territories, to or for the benefit of designated persons or entities unless licensed, authorised or otherwise notified in accordance with the relevant Security Council resolutions.

(d) Countries should have mechanisms for communicating designations to financial institutions and DNFBPs immediately upon taking such action, and providing clear guidance to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms.

(e) Countries should require financial institutions and DNFBPs to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant UNSCRs, including attempted transactions.

(f) Countries should adopt measures which protect the rights of bona fide third parties acting in good faith when implementing the obligations under Recommendation 7.

7.3 Countries should adopt measures for monitoring and ensuring compliance by financial institutions and DNFBPs with the relevant laws or enforceable means governing the obligations under Recommendation 7. Failure to comply with such laws or enforceable means should be subject to civil, administrative or criminal sanctions.

7.4 Countries should develop and implement publicly known procedures to submit de-listing requests to the Security Council in the case of designated persons and entities that, in the view of the country, do not or no longer meet the criteria for designation. These should include:

(a) enabling listed persons and entities to petition a request for de-listing at the Focal Point for de-listing established pursuant to UNSCR 1730, or informing designated persons or entities to petition the Focal Point directly;

(b) publicly known procedures to unfreeze the funds or other assets of persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by a freezing mechanism (i.e. a false positive), upon verification that the person or entity involved is not a designated person or entity;

(c) authorising access to funds or other assets, where countries have determined that the exemption conditions set out in UNSCRs 1718 and 1737 are met, in accordance with the procedures set out in those resolutions; and

(d) mechanisms for communicating de-listings and unfreezings to the financial sector and the DNFBPs immediately upon taking such action, and providing guidance to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations to respect a de-listing or unfreezing action.

7.5 With regard to contracts, agreements or obligations that arose prior to the date on which accounts became subject to targeted financial sanctions:

(a) countries should permit the addition to the accounts frozen pursuant to UNSCRs 1718 or 1737 of interests or other earnings due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of this resolution, provided that any such interest, other earnings and payments continue to

(b) freezing action taken pursuant to UNSCR 1737 should not prevent a designated person or entity from making any payment due under a contract entered into prior to the listing of such person or entity, provided that: (i)the relevant countries have determined that the contract is not related to any of the prohibited items, materials, equipment, goods, technologies, assistance, training, financial assistance, investment, brokering or services referred to in the relevant Security Council resolution; (ii) the relevant countries have determined that the payment is not directly or indirectly

received by a person or entity designated pursuant to UNSCR 1737; and (iii) the relevant countries have submitted prior notification to the 1737 Sanctions Committee of the intention to make or receive such payments or to authorise, where appropriate, the unfreezing of funds, other financial assets or economic resources for this purpose, ten working days prior to such authorisation.

Recommendation 8 – Non-profit organisations (NPOs)

8.1 Countries should:

(a) review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism, including NPOs.

(b) undertake domestic reviews of their NPO sector, or have the capacity to obtain timely information on its activities, size and other relevant features, using all available sources of information, in order to identify the features and types of NPOs that are particularly at risk of being misused for TF or other forms of terrorist support by virtue of their activities or characteristics.

(c) periodically reassess their NPO sector by reviewing new information on the sector's potential vulnerabilities to terrorist activities.

8.2 Countries should conduct outreach to the NPO sector concerning TF issues.

8.3 Countries should have clear policies to promote transparency, integrity, and public confidence in the administration and management of all NPOs.

8.4 Countries should apply the following standards to NPOs which account for (i) a significant portion of the financial resources under the control of the sector; and (ii) a substantial share of the sector's international activities. Such NPOs should be required to:

(a) maintain information on: (i) the purpose and objectives of their stated activities; and (ii) the identity of person(s) who own, control or direct their activities, including senior officers, board members and trustees. This information should be publicly available either directly from the NPO or through appropriate authorities;

(b) issue annual financial statements that provide detailed breakdowns of income and expenditure;

(c) have controls in place to ensure that all funds are fully accounted for, and are spent in a manner that is consistent with the purpose and

objectives of the NPO's stated activities;

(d) be licensed or registered ;

(e) follow a "know your beneficiaries and associated NPOs" rule; and

(f) maintain, for a period of at least five years, records of domestic and international transactions , and the information in (a) and (b) above, and make these available to competent authorities upon appropriate authority.

8.5 Competent authorities should monitor the compliance of NPOs with Criterion 8.4, and should be able to apply proportionate and dissuasive sanctions for violations of the requirements by NPOs or persons acting on behalf of these NPOs.

8.6 Authorities should be able to investigate and gather information on NPOs, including through:

(a) domestic cooperation, coordination and information-sharing among authorities or organisations that hold relevant information on NPOs;

(b) full access to information on the administration and management of particular NPOs (including financial and programmatic information); and

(c) mechanisms to ensure that relevant information is promptly shared with competent authorities, in order to take preventive or investigative action, when there is suspicion or reasonable grounds to suspect that a particular NPO is: a front for fundraising by a terrorist organisation; or being exploited as a conduit for TF, including for the purpose of escaping asset freezing measures; or concealing or obscuring the clandestine diversion of funds intended for legitimate purposes, but redirected for the benefit of terrorists or terrorist organisations.

8.7 Countries should identify appropriate points of contact and procedures to respond to international requests for information regarding particular NPOs suspected of TF or other forms of terrorist support.

Recommendation 9 – Financial Institution Secrecy Laws

9.1 Financial institution secrecy laws should not inhibit the implementation of the FATF Recommendations.

Recommendation 10 - Customer Due Diligence (CDD)

10.1 Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names.

When CDD is required

10.2 Financial institutions should be required to undertake CDD measures when:

(a) establishing business relations;

(b) carrying out occasional transactions above the applicable designated threshold (USD/€ 15,000), including situations where the transaction is carried out in a single operation or in several operations that appear to be linked;

(c) carrying out occasional transactions that are wire transfers in the circumstances covered by Recommendation 16 and its Interpretive Note;

(d) there is a suspicion of ML/TF, regardless of any exemptions or thresholds that are referred to elsewhere under the FATF Recommendations; or

(e) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

Required CDD measures for all customers

10.3 Financial institutions should be required to identify the customer (whether permanent or occasional, and whether natural or legal person or legal arrangement) and verify that customer's identity using reliable, independent source documents, data or information (identification data).

10.4 Financial institutions should be required to verify that any person purporting to act on behalf of the customer is so authorised, and identify and verify

the identity of that person.

10.5 Financial institutions should be required to identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source, such that the financial institution is satisfied that it knows who the beneficial owner is.

10.6 Financial institutions should be required to understand and, as appropriate, obtain information on, the purpose and intended nature of the business relationship.

10.7 Financial institutions should be required to conduct ongoing due diligence on the business relationship, including:

(a) scrutinising transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the financial institution's knowledge of the customer, their business and risk profile, including where necessary, the source of funds; and

(b) ensuring that documents, data or information collected under the CDD process is kept up-to-date and relevant, by undertaking reviews of existing records, particularly for higher risk categories of customers.

Specific CDD measures required for legal persons and legal arrangements

10.8 For customers that are legal persons or legal arrangements, the financial institution should be required to understand the nature of the customer's business and its ownership and control structure.

10.9 For customers that are legal persons or legal arrangements, the financial institution should be required to identify the customer and verify its identity through the following information:

(a) name, legal form and proof of existence;

(b) the powers that regulate and bind the legal person or arrangement, as well as the names of the relevant persons having a senior management position in the legal person or arrangement; and

(c) the address of the registered office and, if different, a principal place of business.

10.10 For customers that are legal persons , the financial institution should be required to identify and take reasonable measures to verify the identity of beneficial owners through the following information:

(a) the identity of the natural person(s) (if any) who ultimately has a controlling ownership interest in a legal person; and

(b) to the extent that there is doubt under (a) as to whether the person(s) with the controlling ownership interest is the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural person(s) (if any) exercising control of the legal person or arrangement through other means; and

(c) where no natural person is identified under (a) or (b) above, the identity of the relevant natural person who holds the position of senior managing official.

10.11 For customers that are legal arrangements, the financial institution should be required to identify and take reasonable measures to verify the identity of beneficial owners through the following information:

(a) for trusts, the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries , and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership);

(b) for other types of legal arrangements, the identity of persons in equivalent or similar positions.

CDD for Beneficiaries of Life Insurance Policies

10.12 In addition to the CDD measures required for the customer and the beneficial owner, financial institutions should be required to conduct the following CDD measures on the beneficiary of life insurance and other investment related insurance policies, as soon as the beneficiary is identified or designated:

(a) for a beneficiary that is identified as specifically named natural or legal persons or legal arrangements – taking the name of the person;

(b) for a beneficiary that is designated by characteristics or by class or by other means – obtaining sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the payout;

(c) for both the above cases – the verification of the identity of the beneficiary should occur at the time of the payout.

10.13 Financial institutions should be required to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable. If the financial institution determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, it should be required to take enhanced measures which should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.

Timing of verification

10.14 Financial institutions should be required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers; or (if permitted) may complete verification after the establishment of the business relationship, provided that:

- *(a) this occurs as soon as reasonably practicable;*
- *(b) this is essential not to interrupt the normal conduct of business; and*
- *(c) the ML/TF risks are effectively managed.*

.

10.15 Financial institutions should be required to adopt risk management procedures concerning the conditions under which a customer may utilise the business relationship prior to verification.

Existing customers

10.16 Financial institutions should be required to apply CDD requirements to existing customers on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

Risk-Based Approach

10.17 Financial institutions should be required to perform enhanced due diligence where the ML/TF risks are higher.

10.18 Financial institutions may only be permitted to apply simplified CDD measures where lower risks have been identified, through an adequate analysis of risks by the country or the financial institution. The simplified measures should be commensurate with the lower risk factors, but are not acceptable whenever there is suspicion of ML/TF, or specific higher risk scenarios apply.

Failure to satisfactorily complete CDD

10.19 Where a financial institution is unable to comply with relevant CDD measures:

(a) it should be required not to open the account, commence business relations or perform the transaction; or should be required to terminate the business relationship; and

(b) it should be required to consider making a suspicious transaction report in relation to the customer.

CDD and tipping-off

10.20 In cases where financial institutions form a suspicion of money laundering or terrorist financing, and they reasonably believe that performing the CDD process will tip-off the customer, they should be permitted not to pursue the CDD process, and instead should be required to file a suspicious transaction report.

Recommendation 11 – Record Keeping

11.1 Financial institutions should be required to maintain all necessary records on transactions, both domestic and international, for at least five years following completion of the transaction.

11.2 Financial institutions should be required to keep all records obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, for at least five years following the termination of the business relationship or after the date of the occasional transaction.

11.3 Transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

11.4 Financial institutions should be required to ensure that all CDD information and transaction records are available swiftly to domestic competent authorities upon appropriate authority.

Recommendation 12 – Politically Exposed Persons (PEPs)

12.1 In relation to foreign PEPs, in addition to performing the CDD measures required under R.10, financial institutions should be required to:

(a) put in place risk management systems to determine whether a customer or the beneficial owner is a PEP;

(b) obtain senior management approval before establishing (or continuing, for existing customers) such business relationships;

(c) take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and

(d) conduct enhanced ongoing monitoring on that relationship.

See Articles 3.1.5, 6.1.3, 6.2 of the AMLCFT law, Articles 7.1, 7.2, 7.3, and 4.2.2 of the draft Regulation on Preventive measure against ML/TF. Reference in the AMLCFT Law to the management of PEPs is at article 6.1.3 which requires transactions conducted in the name of PEPs to be subject to special monitoring in accordance with 6.2 of AMLCFT.

12.2 In relation to domestic PEPs or persons who have been entrusted with a prominent function by an international organisation, in addition to performing the CDD measures required under R.10, financial institutions should be required to:

(a) take reasonable measures to determine whether a customer or the beneficial owner is such a person; and

(b) in cases when there is higher risk business relationship with such a person, adopt the measures in criterion 12.1 (b) to (d).

Where a domestic PEP is identified they are subject to the enhanced CDD required by article 6.2. Articles 7.1, 7.2, 7.3, and 4.2.2 of the draft Regulation on Preventive measure against ML/TF deal with this Recommendation.

12.3 Financial institutions should be required to apply the relevant requirements of criteria 12.1 and 12.2 to family members or close associates of all

types of PEP.

See Article 7.3 of Draft Regulation on Preventive measure against ML/TF.

12.4 In relation to life insurance policies, financial institutions should be required to take reasonable measures to determine whether the beneficiaries and/or, where required, the beneficial owner of the beneficiary, are PEPs. This should occur, at the latest, at the time of the payout. Where higher risks are identified, financial institutions should be required to inform senior management before the payout of the policy proceeds, to conduct enhanced scrutiny on the whole business relationship with the policyholder, and to consider making a suspicious transaction report.

No provisions

Recommendation 13 – Correspondent banking

13.1 In relation to cross-border correspondent banking and other similar relationships, financial institutions should be required to:

(a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business, and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a ML/TF investigation or regulatory action;

(b) assess the respondent institution's AML/CFT controls;

(c) obtain approval from senior management before establishing new correspondent relationships; and

(d) clearly understand the respective AML/CFT responsibilities of each institution.

These requirements are covered by Article 5.6 of the AMLCFT law, Article 8.1 of the draft Regulation on Preventive measure against ML/TF.

13.2 With respect to "payable-through accounts", financial institutions should be required to satisfy themselves that the respondent bank:

(a) has performed CDD obligations on its customers that have direct access to the accounts of the correspondent bank; and

(b) is able to provide relevant CDD information upon request to the correspondent bank.

Article 8.1.6 of the draft Regulation on Preventive measure against ML/TF requires FIs to CDD payable through account thru respondent banks.

13.3 Financial institutions should be prohibited from entering into, or continuing, correspondent banking relationships with shell banks. They should be

required to satisfy themselves that respondent financial institutions do not permit their accounts to be used by shell banks.

Correspondent banking relationships with shell banks is prohibited by Article 5.7 of the AMLCFT Law, article 8.1.7 and 8.1.8 of the draft Regulation on Preventive measure against ML/TF.

Recommendation 15 – New Technologies

15.1 Countries and financial institutions should 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.

Article 5.5 of the AMLCFT Law, Chapter 9 of the draft Regulation on Preventive measure against ML/TF require FIs to "pay special attention to transactions conducted by new or developing technologies and take certain measures to prevent the associated risks of ML and TF that may arise from these transactions.

15.2 Financial institutions should be required to:

(a) undertake the risk assessments prior to the launch or use of such products, practices and technologies; and

(b) take appropriate measures to manage and mitigate the risks.

Chapter 9 of Draft Regulation on Preventive measure against ML/TF require FIs undertake risk assessment prior to launching such new products.

Recommendation 16 – Wire Transfers

Ordering financial institutions

16.1 Financial institutions should be required to ensure that all cross-border wire transfers of USD/EUR 1,000 or more are always accompanied by the following:

(a) Required and accurate originator information:

(i) the name of the originator;

(ii) the originator account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction; and

(iii) the originator's address, or national identity number, or customer identification number, or date and place of birth.

(b) Required beneficiary information:

(i) the name of the beneficiary; and

(ii) the beneficiary account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

Article 5.2.6 of the AMLCFT Law and article 10.1 of the draft Regulation on Preventive measures against ML/TF require FIs to include originator/beneficiary info in Wire transfers.

16.2 Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file should contain required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country; and the financial institution should be required to include the originator's account number or unique transaction reference number.

Article 10.3 of Draft Regulation on Preventive measure against ML/TF deals with this Rec.

16.3 If countries apply a de minimis threshold for the requirements of criterion 16.1, financial institutions should be required to ensure that all cross-border wire transfers below any applicable de minimis threshold (no higher than USD/EUR 1,000) are always accompanied by the following:

(a) Required originator information:

(i) the name of the originator; and

(ii) the originator account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

(b) Required beneficiary information:

(i) the name of the beneficiary; and

(ii) the beneficiary account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

No Threshold is applicable / Not applicable

16.4 The information mentioned in criterion 16.3 need not be verified for accuracy. However, the financial institution should be required to verify the

information pertaining to its customer where there is a suspicion of ML/TF.

No Threshold is applicable / Not applicable

16.5 For domestic wire transfers , the ordering financial institution should be required to ensure that the information accompanying the wire transfer includes originator information as indicated for cross-border wire transfers, unless this information can be made available to the beneficiary financial institution and appropriate authorities by other means.

See Article 10.5 and 10.6 of the draft Regulation on Preventive measure against ML/TF

16.6 Where the information accompanying the domestic wire transfer can be made available to the beneficiary financial institution and appropriate authorities by other means, the ordering financial institution need only be required to include the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary. The ordering financial institution should be required to make the information available within three business days of receiving the request either from the beneficiary financial institution or from appropriate competent authorities. Law enforcement authorities should be able to compel immediate production of such information.

See Article 10.5 and 10.6 of the draft Regulation on Preventive measure against ML/TF.

16.7 The ordering financial institution should be required to maintain all originator and beneficiary information collected, in accordance with Recommendation 11.

See Article 10.9 of the draft Regulation on Preventive measure against ML/TF.

16.8 The ordering financial institution should not be allowed to execute the wire transfer if it does not comply with the requirements specified above at criteria 16.1-16.7.

See Article 10.2 of the draft Regulation on Preventive measure against ML/TF.

Intermediary financial institutions

16.9 For cross-border wire transfers, an intermediary financial institution should be required to ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it.

See Article 10.7 of the draft Regulation on Preventive measure against ML/TF.

16.10 Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, the intermediary financial institution should be required to keep a record, for at least five years, of all the information received from the ordering financial institution or another intermediary financial institution.

See Article 10.7 of the draft Regulation on Preventive measure against ML/TF.

16.11 Intermediary financial institutions should be required to take reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack required originator information or required beneficiary information.

See Article 10.8 of the draft Regulation on Preventive measure against ML/TF.

16.12 Intermediary financial institutions should be required to have risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action.

See article 10.8 of the draft Regulation on Preventive measure against ML/TF.

Beneficiary financial institutions

16.13 Beneficiary financial institutions should be required to take reasonable measures, which may include post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers that lack required originator information or required beneficiary information.

See Article 10.2 of the draft Regulation on Preventive measure against ML/TF.

16.14 For cross-border wire transfers of USD/EUR 1,000 or more, a beneficiary financial institution should be required to verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with Recommendation 11.

See Article 10.9 of the draft Regulation on Preventive measure against ML/TF.

16.15 Beneficiary financial institutions should be required to have risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action.

Article 10.8 of the draft Regulation on Preventive measure against ML/TF

Money or value transfer service operators

16.16 MVTS providers should be required to comply with all of the relevant requirements of R.16 in the countries in which they operate, directly or through their agents.

Money value transfer services are licensed services by the Bank of Mongolia and Financial regulatory committee and regarded as financial services. The MVT licenses have been given only to banks and 4 non bank financial institutions in Mongolia. All these entities with MVT licenses must comply with legal requirements relevant to Recommendation 16 of FATF.

16.17 In the case of a MVTS provider that controls both the ordering and the beneficiary side of a wire transfer, the MVTS provider should be required to:

(a) take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and

Article 7 of the AMLCFT law applies to MVTs.

(b) file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Financial Intelligence Unit.

Article 7 of the AMLCFT law applies to MVTs.

Implementation of Targeted Financial Sanctions

16.18 Countries should ensure that, in the context of processing wire transfers, financial institutions take freezing action and comply with prohibitions from conducting transactions with designated persons and entities, as per obligations set out in the relevant UNSCRs relating to the prevention and suppression of terrorism and terrorist financing, such as UNSCRs 1267 and 1373, and their successor resolutions.

Article 7.1.7 of the Anti terrorism law (freeze without delay) applies to financial institutions, when processing wire transfers.

Recommendation 17 – Reliance on Third Parties

17.1 If financial institutions are permitted to rely on third-party financial institutions and DNFBPs to perform elements (a)-(c) of the CDD measures set out in Recommendation 10 (identification of the customer; identification of the beneficial owner; and understanding the nature of the business) or to introduce business, the ultimate responsibility for CDD measures should remain with the financial institution relying on the third party, which should be required to:

(a) obtain immediately the necessary information concerning elements (a)-(c) of the CDD measures set out in Recommendation 10;

(b) take steps to satisfy itself that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay;

(c) satisfy itself that the third party is regulated, and supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements in line with Recommendations 10 and 11.

Chapter 11 of the draft Regulation on Preventive measure against ML/TF deals with this requirement of recommendation.

17.2 When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.

Chapter 11 of the draft Regulation on Preventive measure against ML/TF with this requirement of recommendation.

17.3 For financial institutions that rely on a third party that is part of the same financial group, relevant competent authorities may also consider that the requirements of the criteria above are met in the following circumstances:

(a) the group applies CDD and record-keeping requirements, in line with Recommendations 10 to 12, and programmes against money laundering and terrorist financing, in accordance with Recommendation 18;

(b) the implementation of those CDD and record-keeping requirements and AML/CFT programmes is supervised at a group level by a competent authority; and

(c) any higher country risk is adequately mitigated by the group's AML/CFT policies.

Chapter 11 of the draft Regulation on Preventive measure against ML/TF with this requirement of recommendation.

Recommendation 18 – Internal Controls and Foreign Branches and Subsidiaries

18.1 Financial institutions should be required to implement programmes against ML/TF, which have regard to the ML/TF risks and the size of the business, and which include the following internal policies, procedures and controls:

(a) compliance management arrangements (including the appointment of a compliance officer at the management level);

(b) screening procedures to ensure high standards when hiring employees;

(c) an ongoing employee training programme; and

(d) an independent audit function to test the system.

Article 14 of AMLCFT Law and Chapter 3 of the draft Regulation on Preventive measures against ML/TF clearly address requirements in this Recommendation.

18.2 Financial groups should be required to implement group-wide programmes against ML/TF, which should be applicable, and appropriate to, all branches and majority-owned subsidiaries of the financial group. These should include the measures set out in criterion 18.1 and also:

(a) policies and procedures for sharing information required for the purposes of CDD and ML/TF risk management;

(b) the provision, at group-level compliance, audit, and/or AML/CFT functions, of customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes; and

(c) adequate safeguards on the confidentiality and use of information exchanged.

Chapter 3 of the draft Regulation on Preventive measures against ML/TF defines measures in this requirement.

18.3 Financial institutions should be required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the home country requirements, where the minimum AML/CFT requirements of the host country are less strict than those of the home country, to the extent that host country laws and regulations permit.

If the host country does not permit the proper implementation of AML/CFT measures consistent with the home country requirements, financial groups should be required to apply appropriate additional measures to manage the ML/TF risks, and inform their home supervisors.

Mongolia does not have any foreign branches of banks or other NBFIs. Not applicable.

Recommendation 19 – Higher Risk Countries

19.1 Financial institutions should be required to apply enhanced due diligence, proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.

Articles 2.2, 2.3.2 and 3.1.3 of the draft Regulation on Preventive measures against ML/TF addresses this requirement.

19.2 Countries should be able to apply countermeasures proportionate to the risks: (a) when called upon to do so by the FATF; and (b) independently of any call by the FATF to do so.

19.3 Countries should have measures in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries.

Article 19.2.3 of the AMLCFT law sets the mechanism empowering the FIU and the BoM to issue guidance to banks on compliance with the Law that is used for this purposes. Article 2.3.2, 3.1.3 and 4.1 of the draft Regulation on Preventive measure against ML/TF also defines measures for this purpose.

Recommendation 20 – Reporting of Suspicious Transactions

20.1 If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to TF, it should be required to report promptly its suspicions to the financial intelligence unit (FIU).

Article 7.2 of AMLCFT Law defines as "If a reporting entity suspects or knows that an asset or transaction or attempted transaction is related to money laundering or terrorism financing or is related to proceeds of crime it shall submit a report to the Financial Information Unit within 24 hours in accordance to the approved by the Financial Information Unit procedures and formats"

Chapter 14 of the draft Regulation on Preventive measure against ML/TF sets the procedures to STR filing.

20.2 Financial institutions should be required to report all suspicious transactions, including attempted transactions, regardless of the amount of the transaction.

STR on attempted transactions are also required by Article 7.2 of AMLCFT Law and Chapter 14 of the draft Regulation on Preventive measure against ML/TF.

Recommendation 21 – Tipping-off and Confidentiality

21.1 Financial institutions and their directors, officers and employees should be protected by law from both criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU. This protection should be available even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

Article 12 of AMLCFT Law, Article 14.22, and 14.23 of the draft Regulation on Preventive measure against ML/TF deals with this requirement.

21.2 Financial institutions and their directors, officers and employees should be prohibited by law from disclosing the fact that a suspicious transaction report or related information is being filed with the FIU.

Article 12 of AMLCFT Law, Article 14.22, and 14.23 of the draft Regulation on Preventive measure against ML/TF deals with this requirement.

Recommendation 22 – Designated Non-Financial Businesses and Professions (DNFBPs): Customer Due Diligence

22.1 DNFBPs should be required to comply with the CDD requirements set out in Recommendation 10 in the following situations:

(a) Casinos – when customers engage in financial transactions equal to or above USD/EUR 3,000.

According to the article 1 of the "Law on prohibition to establish and operate casino" unless otherwise provided by law establishing casino and its operation shall be prohibited in territory of Mongolia.

(b) Real estate agents – when they are involved in transactions for a client concerning the buying and selling of real estate.

Real estate agents are subject to comply with the AMLCFT law (Article 4.1). However, In Mongolia, real estate agents are not involved in transaction for a client concerning the buyng and selling of real estate. Their activities merely include: to advertise real estate and mediate buyers to sellers of real estate.

(c) Dealers in precious metals and dealers in precious stones – when they engage in any cash transaction with a customer equal to or above USD/EUR 15,000.

(d) Lawyers, notaries, other independent legal professionals and accountants when they prepare for, or carry out, transactions for their client concerning the following activities:

- buying and selling of real estate;

- managing of client money, securities or other assets;

- management of bank, savings or securities accounts;

- organisation of contributions for the creation, operation or management of companies;

- creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

Notaries are subject to compliance with the AMLCFT law (Article 4.1) while lawyers and accountants are not. However, all these professionals are not involved in any type of transactions for their client.

(e) Trust and company service providers when they prepare for or carry out transactions for a client concerning the following activities:

- acting as a formation agent of legal persons;

- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;

- providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;

- acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;

- acting as (or arranging for another person to act as) a nominee shareholder for another person.

Mongolia does not have registered trust and company service providers.

22.2 In the situations set out in Criterion 22.1, DNFBPs should be required to comply with the record-keeping requirements set out in Recommendation 11.

22.3 In the situations set out in Criterion 22.1, DNFBPs should be required to comply with the PEPs requirements set out in Recommendation 12.

22.4 In the situations set out in Criterion 22.1, DNFBPs should be required to comply with the new technologies requirements set out in Recommendation 15.

22.5 In the situations set out in Criterion 22.1, DNFBPs should be required to comply with the reliance on third-parties requirements set out in Recommendation 17.

Recommendation 23 – DNFBPs: Other Measures

23.1 The requirements to report suspicious transactions set out in Recommendation 20 should apply to all DNFBPs subject to the following qualifications:

(a) Lawyers, notaries, other independent legal professionals and accountants – when, on behalf of, or for, a client, they engage in a financial

transaction in relation to the activities described in criterion 22.1(d) .

(b) Dealers in precious metals or stones – when they engage in a cash transaction with a customer equal to or above USD/EUR 15,000.

(c) Trust and company service providers – when, on behalf or for a client, they engage in a transaction in relation to the activities described in criterion 22.1(e).

23.2 In the situations set out in criterion 23.1, DNFBPs should be required to comply with the internal controls requirements set out in Recommendation 18.

23.3 In the situations set out in criterion 23.1, DNFBPs should be required to comply with the higher-risk countries requirements set out in Recommendation 19.

23.4 In the situations set out in criterion 23.1, DNFBPs should be required to comply with the tipping-off and confidentiality requirements set out in Recommendation 21.

Recommendation 24 – Transparency and Beneficial Ownership of Legal Persons

24.1 Countries should have mechanisms that identify and describe: (a) the different types, forms and basic features of legal persons in the country; and (b) the processes for the creation of those legal persons, and for obtaining and recording of basic and beneficial ownership information. This information should be publicly available.

According to article 9.1 of Legal entity's state registration law, State registration authority's (GASR) functions are to register legal entity's creation, reorganization, dissolution, also amendments made to its information to state registration, also as stated to this law inform about this through its website, in accordance with regulation stated in this law to issue enquiry from private case of legal entity, to keep record of legal entity's name fund, give enquiry from it, to exchange information with government and non-government organizations.

If enter legal entity's name, identification number to official website of GASR then it is possible to see legal entity's state registration information. To ensure information transparency of legal entity's registration GASR takes relevant measures (develop software, to have direction from relevant authority etc.)

The revised Securities market law requires the identification of the beneficial ownership of companies.

24.2 Countries should assess the ML/TF risks associated with all types of legal person created in the country.

Basic Information

24.3 Countries should require that all companies created in a country are registered in a company registry, which should record the company name, proof of incorporation, legal form and status, the address of the registered office, basic regulating powers, and a list of directors. This information should be publicly available.

In article 10.3 of Legal entity's state registration law stated that "To collect legal entity's private case by digital and paper based form, double record it in state registration database", also in article 11.1 of this law stated that legal entity's private case should include following information:

1.legal entity's name, identification and private case number;

2.legal entity's type, form;

3. official permanent address of legal entity's general administrative, if there is not exists permanent general administrative then permanent address of legal entity who have right to represent legal entity without procurator;

4.about legal entity's creation or reorganization;

5**.information of founders;**

6. documents of creation;

7. information about right succession of each newly created legal entity through reorganization and legal entity where activity stopped;

8. information regarding amendments made to legal entity's information, registered date of it;

9. for companies amount of share capital stated in the documents of creation;

10. legal entity's executive surname, father/mother/'s name, given name, copy of ID card, if foreign citizen foreign investment's identity;

11.if legal entity have branch, representative office then its official permanent address.

In another word above informations of legal entity are registered in digital database also paper based documents are kept in private case.

In article 9.6 of law about legal entity's state registration stated that "All state registration informations except informations stated

in law and regulation about confidential information of State registration authority shall be informed through its official website to public. Informations uploaded to its website would be accepted as official information of State registration authority".

24.4 Companies should be required to maintain the information set out in criterion 24.3, and also to maintain a register of their shareholders or members, containing the number of shares held by each shareholder and categories of shares (including the nature of the associated voting rights). This information should be maintained within the country at a location notified to the company registry.

In article 16.1 of Company law "Company rule is major document of its creation." In article 16.2 stated "Number of announced and issued shares, categories of shares, nominal price, amount of share capital, if announced preferred share number of announced preferred share, its owner's right must be reflected in company's chapter".

According to article 3.1.5 of Law about legal entity's state registration company's chapter is document of its creation and shall register newly approved or revised company chapter, amendment etc within 10 days after adoption of decision and registration to digital database shall be done accordingly every registered time.

24.5 Countries should have mechanisms that ensure that the information referred to in criteria 24.3 and 24.4 is accurate and updated on a timely basis.

In article 13.1 of Law about legal entity's state registration "Unless stated otherwise in law State registration authority shall make decision whether to register foreign invested enterprise or not within 10 days, about other legal entities within 2 working days after the day received complete documents stated in article 17.1-17.3 of this law and to inform about its decision to applicant by letter, by digital form".

Every time when registered new legal entity and amendments made to legal entity's information information would be added to state registration database and database would be updated.

Beneficial Ownership Information

24.6 Countries should use one or more of the following mechanisms to ensure that information on the beneficial ownership of a company is obtained by that company and available at a specified location in their country; or can be otherwise determined in a timely manner by a competent authority:

(a) requiring companies or company registries to obtain and hold up-to-date information on the companies' beneficial ownership;

In article 15.1 of Company law stated that "Relevant documents shall be submitted to registration authority in order to register company in state registration within 30 days after approval of decision about company creation",

In 17.4 "Amendment of company rule, revised version of company rule shall be registered within 10 days after its decision in accordance with

regulation stated in law."

In 17.5 "Registration authority after the receipt of documents stated in article 17.3 of Company law shall make reasonable decision whether to register or not amendment, revised version of company rule to state registration within 2 working days."

(b) requiring companies to take reasonable measures to obtain and hold up-to-date information on the companies' beneficial ownership;

Article 11 of Law about legal entity's state registration requires all information

If amendment are made to information stated in article 11.1 of this law then relevant legal entity have obligation to inform about this within 15 days to state registration authority and in article 27.5 of this law states that if legal entity haven't registered information amendment within duration stated in article 11.3 of this law judge or competent state inspector according to offence type shall impose penalty equal with amount of 1 month minimum wage one to three more times.

(c) using existing information, including: (i) information obtained by financial institutions and/or DNFBPs, in accordance with Recommendations 10 and 22; (ii) information held by other competent authorities on the legal and beneficial ownership of companies; (iii) information held by the company as required in criterion 24.3 above; and (iv) available information on companies listed on a stock exchange, where disclosure requirements ensure adequate transparency of beneficial ownership.

24.7 Countries should require that the beneficial ownership information is accurate and as up-to-date as possible.

24.8 Countries should ensure that companies cooperate with competent authorities to the fullest extent possible in determining the beneficial owner, by:

(a) requiring that one or more natural persons resident in the country is authorised by the company , and accountable to competent authorities, for providing all basic information and available beneficial ownership information, and giving further assistance to the authorities; and/or

(b) requiring that a DNFBP in the country is authorised by the company, and accountable to competent authorities, for providing all basic information and available beneficial ownership information, and giving further assistance to the authorities; and/or

(c) taking other comparable measures, specifically identified by the country.

24.9 All the persons, authorities and entities mentioned above, and the company itself (or its administrators, liquidators or other persons involved in the dissolution of the company), should be required to maintain the information and records referred to for at least five years after the date on which the company is dissolved or otherwise ceases to exist, or five years after the date on which the company ceases to be a customer of the professional intermediary

or the financial institution.

Other Requirements

24.10 Competent authorities, and in particular law enforcement authorities, should have all the powers necessary to obtain timely access to the basic and beneficial ownership information held by the relevant parties.

24.11 Countries that have legal persons able to issue bearer shares or bearer share warrants should apply one or more of the following mechanisms to ensure that they are not misused for money laundering or terrorist financing:

(a) prohibiting bearer shares and share warrants; or

(b) converting bearer shares and share warrants into registered shares or share warrants (for example through dematerialisation); or

(c) immobilising bearer shares and share warrants by requiring them to be held with a regulated financial institution or professional intermediary; or

(d) requiring shareholders with a controlling interest to notify the company, and the company to record their identity; or

(e) using other mechanisms identified by the country.

24.12 Countries that have legal persons able to have nominee shares and nominee directors should apply one or more of the following mechanisms to ensure they are not misused:

(a) requiring nominee shareholders and directors to disclose the identity of their nominator to the company and to any relevant registry, and for this information to be included in the relevant register; or

(b) requiring nominee shareholders and directors to be licensed, for their nominee status to be recorded in company registries, and for them to maintain information identifying their nominator, and make this information available to the competent authorities upon request. ; or

(c) using other mechanisms identified by the country.

24.13 There should be liability and proportionate and dissuasive sanctions, as appropriate for any legal or natural person that fails to comply with the requirements.

24.14 Countries should rapidly provide international cooperation in relation to basic and beneficial ownership information, on the basis set out in Recommendations 37 and 40. This should include:

(a) facilitating access by foreign competent authorities to basic information held by company registries;

In article 15.2 of the General law for state registration stated that state registration authority shall provide relevant enquiry, information to its organization function according to the request of competent official of law enforcement and other authorized government organization.

General authority for state registration electronically exchanges information about legal entity's registration with General Police Authority, Anti-corruption agency, General department of taxation, General executive agency of court decision, and the General authority for border protection.

(b) exchanging information on shareholders; and

(c) using their competent authorities' investigative powers, in accordance with their domestic law, to obtain beneficial ownership information on behalf of foreign counterparts.

24.15 Countries should monitor the quality of assistance they receive from other countries in response to requests for basic and beneficial ownership information or requests for assistance in locating beneficial owners residing abroad.

Recommendation 25 – Transparency and Beneficial Ownership of Legal Arrangements

25.1 Countries should require:

(a) trustees of any express trust governed under their law to obtain and hold adequate, accurate, and current information on the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust;

(b) trustees of any trust governed under their law to hold basic information on other regulated agents of, and service providers to, the trust, including investment advisors or managers, accountants, and tax advisors; and

(c) professional trustees to maintain this information for at least five years after their involvement with the trust ceases.

25.2 Countries should require that any information held pursuant to this Recommendation is kept accurate and as up to date as possible, and is updated

on a timely basis.

25.3 All countries should take measures to ensure that trustees disclose their status to financial institutions and DNFBPs when forming a business relationship or carrying out an occasional transaction above the threshold.

25.4 Trustees should not be prevented by law or enforceable means from providing competent authorities with any information relating to the trust; or from providing financial institutions and DNFBPs, upon request, with information on the beneficial ownership and the assets of the trust to be held or managed under the terms of the business relationship.

25.5 Competent authorities, and in particular law enforcement authorities, should have all the powers necessary to be able to obtain timely access to information held by trustees, and other parties (in particular information held by financial institutions and DNFBPs), on the beneficial ownership and control of the trust, including: (a) the beneficial ownership; (b) the residence of the trustee; and (c) any assets held or managed by the financial institution or DNFBP, in relation to any trustees with which they have a business relationship, or for which they undertake an occasional transaction.

25.6 Countries should rapidly provide international cooperation in relation to information, including beneficial ownership information, on trusts and other legal arrangements, on the basis set out in Recommendations 37 and 40. This should include:

(a) facilitating access by foreign competent authorities to basic information held by registries or other domestic authorities;

It is possible to exchange information about legal entities with overseas government organizations which have same function as ours.

For example: GASR and State registration chamber under the Ministry of Justice of Russian Federation concluded “Memorandum of understanding” in December 2010 and agreed to mutually support its activity and exchange information.

(b) exchanging domestically available information on the trusts or other legal arrangement; and

General authority for state registration in accordance with agreement electronically exchanges state registration information about company and NPO with General Police Authority, Anti-corruption agency, General department of taxation, General executive agency of court decision, and the General authority for border protection.

(c) using their competent authorities’ investigative powers, in accordance with domestic law, in order to obtain beneficial ownership information on behalf of foreign counterparts.

25.7 Countries should ensure that trustees are either (a) legally liable for any failure to perform the duties relevant to meeting their obligations; or (b) that there are proportionate and dissuasive sanctions, whether criminal, civil or administrative, for failing to comply.

25.8 Countries should ensure that there are proportionate and dissuasive sanctions, whether criminal, civil or administrative, for failing to grant to competent authorities timely access to information regarding the trust referred to in criterion 25.1.

Recommendation 26 – Regulation and Supervision of Financial Institutions

26.1 Countries should designate one or more supervisors that have responsibility for regulating and supervising (or monitoring) financial institutions' compliance with the AML/CFT requirements.

Supervision authorities have been expanded from FIU to Banking supervision department of BOM, Financial regulatory Commission (FRC) and FIU by Article 19.1 of the revised AML/CFT Law on 31 of May 2013. Banking supervision department of BOM is responsible for AML/CFT supervision of banks which is regulated through "Onsite superivision of AML/CFT regulation of banks" and "Offsite supervision of AML/CFT regulation of Banks" both approved on December 25, 2015 and FRC is responsible for AML/CFT supervision of NBFI, Insurance companies, licensed securities market entities, Investment funds, savings and credit cooperatives which is regulated by "AML/CFT supervision regulation to non banking reporting entities" which was approved in 2009. FRC has its power to regulate entities according to the Law on Legal status of FRC (Provision 1.1)

Technical assistance to enhance AML/CFT supervision framework was given by IMF with total of 8 missions from 2012 to 2016. During the technical assistance, the AMLCFT offsite risk assessment tools and onsite examination procedures were developed both by BOM and FRC.

- BOM – An AML/CFT risk assessment tool is attached to the offsite supervision regulation and examination of onsite procedures were attached onsite supervision regulation and supervision handbook. These developments are tested and implemented by supervisors of banking supervision department and FIU supervisors of BOM.
- FRC – phase II of the TA assistance of IMF is given to FRC from 2015. Both offsite tool and onsite examinations were also developed as well and these developments are in the testing and fine tuning period. Developments are recommended to be approved by mid 2016 by IMF mission report in April 2016.

Market Entry

26.2 Core Principles financial institutions should be required to be licensed. Other financial institutions, including those providing a money or value

transfer service or a money or currency changing service, should be licensed or registered. Countries should not approve the establishment, or continued operation, of shell banks.

Article 6 and 18 of Banking Law; Provision 7.1.6 of The Non Banking Institutions law. FRC has right to issue licenses to the applied non financial instututions according to the Provision 22.1 of Law on Legal status of FRC.

26.3 Competent authorities or financial supervisors should take the necessary legal or regulatory measures to prevent criminals or their associates from holding (or being the beneficial owner of) a significant or controlling interest, or holding a management function, in a financial institution.

Risk-based approach to supervision and monitoring

26.4 Financial institutions should be subject to:

(a) for core principles institutions - regulation and supervision in line with the core principles , where relevant for AML/CFT, including the application of consolidated group supervision for AML/CFT purposes.

(b) for all other financial institutions - regulation and supervision or monitoring, having regard to the ML/TF risks in that sector. At a minimum, for financial institutions providing a money or value transfer service, or a money or currency changing service - systems for monitoring and ensuring compliance with national AML/CFT requirements.

Banking Law, Regulation on onsite supervision on banks (2015), Regulation on offsite supervision on banks (2015), AMLCFT Supervisory Handbook (2015), Risk assessment tools (2016) enable supervision accordign to these requirements.

26.5 The frequency and intensity of on-site and off-site AML/CFT supervision of financial institutions or groups should be determined on the basis of:

(a) the ML/TF risks and the policies, internal controls and procedures associated with the institution or group, as identified by the supervisor's assessment of the institution's or group's risk profile;

(b) the ML/TF risks present in the country; and

(c) the characteristics of the financial institutions or groups, in particular the diversity and number of financial institutions and the degree of discretion allowed to them under the RBA.

Article 1.2 of Regulation on onsite supervision on banks, and Article 1.2.2 of Regulation on offsite supervision on banks, Supervisory

Handbook, Risk assessment tools address this requirement. Risk assessment of banks and other reporting entities are conducted twice a year through data collection template from respective entities. All this developments cover areas in this section. These procedures are part of offsite control. Onsite supervision is conducted based on the strategy which reflects offsite analysis report and risk profile of the entities.

26.6 The supervisor should review the assessment of the ML/TF risk profile of a financial institution or group (including the risks of non-compliance) periodically, and when there are major events or developments in the management and operations of the financial institution or group.

Regulation on onsite supervision on banks (2015), Regulation on offsite supervision on banks (2015), Supervisory Handbook, Risk assessment tools

Recommendation 27 – Powers of Supervisors

27.1 Supervisors should have powers to supervise or monitor and ensure compliance by financial institutions with AML/CFT requirements.

Article 18.2, 19.2, 19.2.2, 19.2.3 of Banking Law and Regulation on onsite supervision on banks (2015), Article 19 of the AMLCFT law, Regulation on offsite supervision on banks (2015) give broad powers to supervision. The Article 25 of the Law on legal status of FRC of 2005, the Article of Rule of Inspector of FRC of 2015 indicate the FRC inspectors' powers and authorities.

27.2 Supervisors should have the authority to conduct inspections of financial institutions.

Article 19 of the AMLCFT law, Regulation on onsite supervision on banks (2015), Regulation on offsite supervision on banks (2015) and AML/CFT supervision regulation of non banking entities also provides such powers. Supervisors of FRC have such powers in the respective law of reporting entities.

27.3 Supervisors should be authorised to compel production of any information relevant to monitoring compliance with the AML/CFT requirements.

Supervisors of the BOM have authority of state inspectors by article 24 and 25 of Central banking law and supervisors of FIU have this authority by article 16.7 of AML/CFT law. In addition to that "state inpectors rule" gives power to compel production of any information related to AMLCFT supervision. Regulation on onsite supervision on banks (2015), Regulation on offsite supervision on banks (2015) and AML/CFT supervision regulation of non banking entities also provide such powers.

27.4 Supervisors should be authorised to impose sanctions in line with Recommendation 35 for failure to comply with the AML/CFT requirements. This should include powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the financial institution's licence.

Article 7.10 of the Administrative Violations law provides power to impose sanctions for failure of compliance in all reporting entities.

Recommendation 28 – Regulation and Supervision of DNFBPs

Casinos

28.1 Countries should ensure that casinos are subject to AML/CFT regulation and supervision. At a minimum:

(a) Countries should require casinos to be licensed.

(b) Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding (or being the beneficial owner of) a significant or controlling interest, or holding a management function, or being an operator of a casino.

(c) Casinos should be supervised for compliance with AML/CFT requirements.

DNFBPs other than casinos

28.2 There should be a designated competent authority or self-regulatory body (SRB) responsible for monitoring and ensuring compliance of DNFBPs with AML/CFT requirements.

28.3 Countries should ensure that the other categories of DNFBPs are subject to systems for monitoring compliance with AML/CFT requirements.

28.4 The designated competent authority or SRB should:

(a) have adequate powers to perform its functions, including powers to monitor compliance;

(b) take the necessary measures to prevent criminals or their associates from being professionally accredited, or holding (or being the beneficial owner of) a significant or controlling interest, or holding a management function in a DNFBP; and

(c) have sanctions available in line with Recommendation 35 to deal with failure to comply with AML/CFT requirements.

All DNFBPs

28.5 Supervision of DNFBPs should be performed on a risk-sensitive basis, including:

(a) determining the frequency and intensity of AML/CFT supervision of DNFBPs on the basis of their understanding of the ML/TF risks, taking into

consideration the characteristics of the DNFBPs, in particular their diversity and number; and

(b) taking into account the ML/TF risk profile of those DNFBPs, and the degree of discretion allowed to them under the RBA, when assessing the adequacy of the AML/CFT internal controls, policies and procedures of DNFBPs.

Recommendation 29 – Financial Intelligence Unit (FIU)

29.1 Countries should establish a FIU with responsibility for acting as a national centre for receipt and analysis of suspicious transaction reports and other information relevant to money laundering, associated predicate offences and terrorist financing; and for the dissemination of the results of that analysis.

Mongolia approved the law on AML/CFT on July 6, 2006 and revised it in May 31, 2013. In accordance with this law, the Financial Information (intelligence) unit (FIU) was established on November 29, 2006 within the structure of the Bank of Mongolia (Article 16.2). Mongolian FIU is an administrative type of FIU and does not have any investigative power. As stipulated in Article 18.1.1 and Article 18.1.2 of the AML/CFT law, the FIU of Mongolia is the national center to receive and collect financial transaction information from reporting entities stated in Article 4.1 of this law, to conduct analysis, and to disseminate information to the relevant law enforcement agencies if there are sufficient grounds to suspect that information has the purpose of or related to money laundering or terrorism financing.

29.2 The FIU should serve as the central agency for the receipt of disclosures filed by reporting entities, including:

(a) suspicious transaction reports filed by reporting entities as required by Recommendation 20 and 23; and

The Mongolian FIU is established pursuant to Article 16.1 of the AML/CFT law as an autonomous and independent agency that serves as the central agency for the receipt of suspicious transaction reports (STRs) filed by reporting entities in accordance with Article 7.2 of the AML/CFT law.

Pursuant to Article 7.2 of the AML/CFT law, STRs are submitted to the FIU within 24 hours in respect of a financial transaction that occurs or is attempted, and for which there are reasonable grounds to suspect that the transaction is related to money laundering or terrorist financing or the proceeds of crime. For STRs, there is no threshold amount unlike all other reporting obligations.

(b) any other information as required by national legislation (such as cash transaction reports, wire transfers reports and other threshold-based declarations/disclosures).

The Mongolian FIU serves as the central agency for the receipt of cash transaction reports (CTRs) and foreign settlement transactions (FSTRs) filed by reporting entities as stipulated in Article 7.1 of the AML/CFT law.

CTRs are submitted to the FIU within 5 working days when a reporting entity conducts a transaction of 20 million togrog (equivalent foreign currency) or more in cash made by, or on behalf of, an individual or entity in compliance with the Regulation on Reporting Information to FIU (Article 3.1.1).

Pursuant to Article 7.1 of the AML/CFT law and Article 3.1.3 of the Regulation on Reporting Information to FIU, foreign settlement transaction reports (FSTRs) are submitted to the FIU within 5 working days when a reporting entity performs a foreign transaction of 20 million togrog (equivalent foreign currency) or more out of or into Mongolia made by, or on behalf of, an individual or entity.

In addition, the Bank of Mongolia made an agreement with the Mongolian Customs Agency in January 2009 in order to implement Article 15.2 of the AML/CFT law and to establish a system for control of cross border movements of cash. A system where declaration forms to be filled in by carriers of cash equivalent to 15 million togrog (equivalent foreign currency) or more has been in place in the border areas since January 2009.

29.3 The FIU should:

(a) in addition to the information that entities report to the FIU, be able to obtain and use additional information from reporting entities, as needed to perform its analysis properly; and

Article 4 of the Regulation on Reporting Information to FIU enables the FIU to make requests of and obtain additional information from reporting entities as needed to conduct STR analysis.

The FIU can obtain and use additional information in relation to STRs, CTRs, and FSTRs submitted by reporting entities upon request to perform its analysis properly. If additional information is related to STRs, CTRs, and/or FSTRs that were submitted by a reporting entity itself, the FIU sends an email request. If additional information is related to reports sent by a different reporting entity or different source of information, the FIU sends an official request signed by the head of FIU to a reporting entity. Reporting entities reply with additional information within 1 to 5 working days depending on information volume (Article 4, Regulation on Reporting Information to FIU).

(b) have access to the widest possible range of financial, administrative and law enforcement information that it requires to properly undertake its functions.

As set forth by Article 18.5 of the AML/CFT law, the FIU has a power to obtain information on state registration, property registration, social insurance registration, border crossing registration, investment registration, and records of transactions made between banks from corresponding competent authorities for the purposes of properly undertaking its functions prescribed in the law. The FIU extensively facilitate

open and public information sources for the purposes of STR analysis.

29.4 The FIU should conduct:

(a) operational analysis, which uses available and obtainable information to identify specific targets, to follow the trail of particular activities or transactions, and to determine links between those targets and possible proceeds of crime, money laundering, predicate offences and terrorist financing; and

One of the core functions of the FIU as stipulated in Article 18 of the AML/CFT law is to analyze information received and held by the FIU in relation to money laundering, financing of terrorism and the proceeds of crime. In this regard, in 2011, the FIU issued an internal Guideline on Conducting STR Analysis.

(b) strategic analysis, which uses available and obtainable information, including data that may be provided by other competent authorities, to identify money laundering and terrorist financing related trends and patterns.

The FIU's ability to undertake strategic analysis is currently limited. However, an internal Guideline on Conducting Strategic Analysis is being developed and new IT tools that will considerably enhance the FIU's ability to conduct strategic analysis are also being developed. Job description of one staff member of FIU is dedicated to strategic analysis.

29.5 The FIU should be able to disseminate, spontaneously and upon request, information and the results of its analysis to relevant competent authorities, and should use dedicated, secure and protected channels for the dissemination.

The FIU of Mongolia is authorized by Article 18.1.2 of the AML/CFT law to disseminate information and the results of its analysis either spontaneously or on request to competent law enforcement authorities and anti-terrorism agencies, when there are sufficient grounds to suspect that a transaction is or might be related to money laundering or financing of terrorism.

29.6 The FIU should protect information by:

(a) having rules in place governing the security and confidentiality of information, including procedures for handling, storage, dissemination, and protection of, and access to, information;

The FIU protects its information as follows: Article 13.1 of the AML/CFT law prohibits reporting entities and the FIU from disclosing information except in cases specified in the law. Additionally, pursuant to Article 13.2 of the AML/CFT law, all FIU staff must not disclose confidential information related to customers' transactions other than for purposes authorised by the AML/CFT law. This applies even after the end of staff's tenure. The FIU has also internal policies and regulations for staff who have an obligation to handle, store, disseminate, and access to and

protect of information.

"Regulation on Procedures for Receiving, Transferring and Analysing Financial Transaction Reports" outlines procedures for receiving, registering, storing and disseminating information. "Regulation on Security of the FIU" outlines procedures for handling, storing, securing and protecting of information, whilst "Secrecy procedure of the FIU" outlines procedures for handling, accessing to, storing, disseminating, and protecting of the FIU's confidential information.

(b) ensuring that FIU staff members have the necessary security clearance levels and understanding of their responsibilities in handling and disseminating sensitive and confidential information; and

Since staff members of the FIU are all public servants, before being hired to BOM, they are required to pass security and conflict of interest clearance, Police criminal record database check, and IAAC checks for conflicts of interest. All FIU staff members are required, not only during their tenure, but also after their retirement, to keep what they learned in the course of their duties confidential (Article 13.2 AML/CFT law). According to Article 6.6 of "Secrecy procedure of the FIU", all persons acquainted with the FIU secrets or confidential information through his/her work function and/or professional duties issue a written guarantee to not to disclose the FIU secrets or confidential information and will be liable for any disclosure.

(c) ensuring that there is limited access to its facilities and information, including information technology systems.

"Regulation on security of the FIU" provides procedures to be followed for access to FIU's IT systems. All FIU staff and other IT staff from BOM must follow this regulation in duties including reviewing, developing, using, repairing and managing the computers, devices and software that used to store, transmit, use and organize data and information for the use of the FIU.

29.7 The FIU should be operationally independent and autonomous, by:

(a) having the authority and capacity to carry out its functions freely, including the autonomous

The Mongolian FIU is established pursuant to Article 16.1 of the AML/CFT law as an autonomous and independent agency. The Governor of the Bank of Mongolia, in consultation with the head of the competent law enforcement authority, appoints and may dismiss the head of Mongolian FIU. The FIU is established within the Bank of Mongolia and the organisational structure, operational and strategic plans and the budget of the FIU are approved by the Governor of the Bank of Mongolia. Although the FIU is located within the Bank of Mongolia's structure, the full operational autonomy and independence is established by Article 16.1 of the AML/CFT law and by the FIU Chapter which was approved in May 7, 2007 (Article 2.2.)

In accordance with the "Regulation on Procedures for Receiving, Transferring and Analysing Financial Transaction Reports" the FIU makes decisions autonomously to analyse, request and/or forward or disseminate specific information.

(b) being able to make arrangements or engage independently with other domestic competent authorities or foreign counterparts on the exchange of information;

Articles 21 and 18.1.1 of the AML/CFT law permit cooperation with foreign and international organizations with similar functions. This allows the exchange of information with foreign counterpart FIUs and other organisations.

Article 18.1.1 of the AMLCFT law allows the FIU to receive or collect information from databases of local and foreign institutions.

Further, Article 19.2.4 of the AMLCFT law allows the FIU to "cooperate with and exchange information with other competent authorities and provide assistance in investigations, prosecutions, or proceedings related to money laundering or terrorism financing".

(c) when it is located within the existing structure of another authority, having distinct core functions from those of the other authority; and

Although the FIU is located within the structure of the Bank of Mongolia, the FIU has distinct core functions from the Bank of Mongolia as established by Article 18 of the AML/CFT law.

(d) being able to obtain and deploy the resources needed to carry out its functions, on an individual or routine basis, free from any undue political, government or industry influence or interference, which might compromise its operational independence.

Article 16.3 of the AML/CFT law states that the budget of the FIU is to be proposed by the Cooperation Council and approved by the Governor of the Bank of Mongolia. The Cooperation Council is established by Article 22 of the AML/CFT law and consists of representatives of all ministries and agencies having a stake in Mongolia's AML/CFT framework. The involvement of the Cooperation Council in the recommendation of the FIU budget ensures that FIU budget decisions are made in a transparent fashion.

29.8 Where a country has created an FIU and is not an Egmont Group member, the FIU should apply for membership in the Egmont Group. The FIU should submit an unconditional application for membership to the Egmont Group and fully engage itself in the application process.

Mongolian FIU applied for a membership in the Egmont Group in 2007 and the membership was approved at Egmont Annual Meeting in May, 2009 in Doha, Qatar. Since then, Mongolian FIU has been actively participating in Operational Working Group of the Egmont Group.

Recommendation 30 – Responsibilities of Law Enforcement and Investigative Authorities

30.1 There should be designated law enforcement authorities that have responsibility for ensuring that money laundering, associated predicate offences and terrorist financing offences are properly investigated, within the framework of national AML/CFT policies.

30.2 Law enforcement investigators of predicate offences should either be authorised to pursue the investigation of any related ML/TF offences during a parallel financial investigation, or be able to refer the case to another agency to follow up with such investigations, regardless of where the predicate offence occurred.

30.3 There should be one or more designated competent authorities to expeditiously identify, trace, and initiate freezing and seizing of property that is, or may become, subject to confiscation, or is suspected of being proceeds of crime.

30.4 Countries should ensure that Recommendation 30 also applies to those competent authorities, which are not law enforcement authorities, per se, but which have the responsibility for pursuing financial investigations of predicate offences, to the extent that these competent authorities are exercising functions covered under Recommendation 30.

30.5 If anti-corruption enforcement authorities are designated to investigate ML/TF offences arising from, or related to, corruption offences under Recommendation 30, they should also have sufficient powers to identify, trace, and initiate freezing and seizing of assets.

Recommendation 31 – Powers of Law Enforcement and Investigative Authorities

31.1 Competent authorities conducting investigations of money laundering, associated predicate offences and terrorist financing should be able to obtain access to all necessary documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for:

(a) the production of records held by financial institutions, DNFBPs and other natural or legal persons;

(b) the search of persons and premises;

(c) taking witness statements; and

(d) seizing and obtaining evidence.

31.2 Competent authorities conducting investigations should be able to use a wide range of investigative techniques for the investigation of money laundering, associated predicate offences and terrorist financing, including:

(a) undercover operations;

(b) intercepting communications;

(c) accessing computer systems; and

(d) controlled delivery.

31.3 Countries should have mechanisms in place:

(a) to identify, in a timely manner, whether natural or legal persons hold or control accounts; and

(b) to ensure that competent authorities have a process to identify assets without prior notification to the owner.

31.4 Competent authorities conducting investigations of money laundering, associated predicate offences and terrorist financing should be able to ask for

all relevant information held by the FIU.

Recommendation 32 – Cash Couriers

32.1 Countries should implement a declaration system or a disclosure system for incoming and outgoing cross-border transportation of currency and bearer negotiable instruments (BNIs). Countries should ensure that a declaration or disclosure is required for all physical cross-border transportation, whether by travellers or through mail and cargo, but may use different systems for different modes of transportation.

32.2 In a declaration system, all persons making a physical cross-border transportation of currency or BNIs, which are of a value exceeding a pre-set, maximum threshold of USD/EUR 15,000, should be required to submit a truthful declaration to the designated competent authorities. Countries may opt from among the following three different types of declaration system:

(a) A written declaration system for all travellers;

(b) A written declaration system for all travellers carrying amounts above a threshold; and/or

(c) An oral declaration system for all travellers.

32.3 In a disclosure system, travellers should be required to give a truthful answer and provide the authorities with appropriate information upon request, but are not required to make an upfront written or oral declaration.

32.4 Upon discovery of a false declaration or disclosure of currency or BNIs or a failure to declare or disclose them, designated competent authorities should have the authority to request and obtain further information from the carrier with regard to the origin of the currency or BNIs, and their intended use.

32.5 Persons who make a false declaration or disclosure should be subject to proportionate and dissuasive sanctions, whether criminal, civil or administrative.

32.6 Information obtained through the declaration/disclosure process should be available to the FIU either through: (a) a system whereby the FIU is notified about suspicious cross-border transportation incidents; or (b) by making the declaration/disclosure information directly available to the FIU in some other way.

32.7 At the domestic level, countries should ensure that there is adequate co-ordination among customs, immigration and other related authorities on issues related to the implementation of Recommendation 32.

32.8 Competent authorities should be able to stop or restrain currency or BNIs for a reasonable time in order to ascertain whether evidence of ML/TF may be found in cases:

(a) where there is a suspicion of ML/TF or predicate offences; or

(b) where there is a false declaration or false disclosure.

32.9 Countries should ensure that the declaration/disclosure system allows for international co-operation and assistance, in accordance with Recommendations 36 to 40. To facilitate such co-operation, information shall be retained when:

(a) a declaration or disclosure which exceeds the prescribed threshold is made; or

(b) there is a false declaration or false disclosure; or

(c) there is a suspicion of ML/TF.

32.10 Countries should ensure that strict safeguards exist to ensure proper use of information collected through the declaration/disclosure systems, without restricting either: (i) trade payments between countries for goods and services; or (ii) the freedom of capital movements, in any way.

32.11 Persons who are carrying out a physical cross-border transportation of currency or BNIs that are related to ML/TF or predicate offences should be subject to: (a) proportionate and dissuasive sanctions, whether criminal, civil or administrative; and (b) measures consistent with Recommendation 4 which would enable the confiscation of such currency or BNIs.

Recommendation 33 – Statistics

33.1 Countries should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/CFT systems. This should include keeping statistics on:

(a) Suspicious transaction reports, received and disseminated;

(b) ML/TF investigations, prosecutions and convictions;

(c) Property frozen; seized and confiscated; and

(d) Mutual legal assistance or other international requests for co-operation made and received.

Recommendation 34 – Guidance and Feedback

34.1 Competent authorities, supervisors, and SRBs should establish guidelines and provide feedback, which will assist financial institutions and DNFBPs in applying national AML/CFT measures, and in particular, in detecting and reporting suspicious transactions.

Recommendation 35 – Sanctions

35.1 Countries should ensure that there is a range of proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with natural or legal persons that fail to comply with the AML/CFT requirements of Recommendations 6, and 8 to 23.

35.2 Sanctions should be applicable not only to financial institutions and DNFBPs but also to their directors and senior management.

Recommendation 36 – International Instruments

36.1 Countries should become a party to the Vienna Convention, the Palermo Convention, the United Nations Convention against Corruption (the Merida Convention) and the Terrorist Financing Convention.

36.2 Countries should fully implement the Vienna Convention, the Palermo Convention, the Merida Convention and the Terrorist Financing Convention.

Recommendation 37 – Mutual Legal Assistance

37.1 Countries should have a legal basis that allows them to rapidly provide the widest possible range of mutual legal assistance in relation to money laundering, associated predicate offences and terrorist financing investigations, prosecutions and related proceedings.

37.2 Countries should use a central authority, or another established official mechanism, for the transmission and execution of requests. There should be clear processes for the timely prioritisation and execution of mutual legal assistance requests. To monitor progress on requests, a case management system

should be maintained.

37.3 Mutual legal assistance should not be prohibited or made subject to unreasonable or unduly restrictive conditions.

37.4 Countries should not refuse a request for mutual legal assistance:

(a) on the sole ground that the offence is also considered to involve fiscal matters; or

(b) on the grounds of secrecy or confidentiality requirements on financial institutions [or DNFBPs], except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies.

37.5 Countries should maintain the confidentiality of mutual legal assistance requests that they receive and the information contained in them, subject to fundamental principles of domestic law, in order to protect the integrity of the investigation or inquiry.

37.6 Where mutual legal assistance requests do not involve coercive actions, countries should not make dual criminality a condition for rendering assistance.

37.7 Where dual criminality is required for mutual legal assistance, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

37.8 Powers and investigative techniques that are required under R.31 or otherwise available to domestic competent authorities should also be available for use in response to requests for mutual legal assistance, and, if consistent with the domestic framework, in response to a direct request from foreign judicial or law enforcement authorities to domestic counterparts. These should include:

(a) all of the specific powers required under R.31 relating to the production, search and seizure of information, documents, or evidence (including financial records) from financial institutions, or other natural or legal persons, and the taking of witness statements; and

(b) a broad range of other powers and investigative techniques.

Recommendation 38 – Mutual Legal Assistance: Freezing and Confiscation

38.1 Countries should have the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize, or confiscate:

(a) laundered property from,

(b) proceeds from,

(c) instrumentalities used in, or

(d) instrumentalities intended for use in, money laundering, predicate offences, or terrorist financing; or

(e) property of corresponding value.

38.2 Countries should have the authority to provide assistance to requests for cooperation made on the basis of non-conviction based confiscation proceedings and related provisional measures, at a minimum in circumstances when a perpetrator is unavailable by reason of death, flight, absence, or the perpetrator is unknown, unless this is inconsistent with fundamental principles of domestic law.

38.3 Countries should have: (a) arrangements for co-ordinating seizure and confiscation actions with other countries; and (b) mechanisms for managing, and when necessary disposing of, property frozen, seized or confiscated.

38.4 Countries should be able to share confiscated property with other countries, in particular when confiscation is directly or indirectly a result of co-ordinated law enforcement actions.

Recommendation 39 – Extradition

39.1 Countries should be able to execute extradition requests in relation to ML/TF without undue delay. In particular, countries should:

(a) ensure ML and TF are extraditable offences;

(b) ensure that they have a case management system, and clear processes for the timely execution of extradition requests including prioritisation

where appropriate; and

(c) not place unreasonable or unduly restrictive conditions on the execution of requests.

39.2 Countries should either:

(a) extradite their own nationals; or

(b) where they do not do so solely on the grounds of nationality, should, at the request of the country seeking extradition, submit the case without undue delay to its competent authorities for the purpose of prosecution of the offences set forth in the request.

39.3 Where dual criminality is required for extradition, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

39.4 Consistent with fundamental principles of domestic law, countries should have simplified extradition mechanisms in place.

Recommendation 40 – Other Forms of International Cooperation

General Principles

40.1 Countries should ensure that their competent authorities can rapidly provide the widest range of international cooperation in relation to money laundering, associated predicate offences and terrorist financing. Such exchanges of information should be possible both spontaneously and upon request.

40.2 Competent authorities should:

(a) have a lawful basis for providing cooperation;

(b) be authorised to use the most efficient means to cooperate;

(c) have clear and secure gateways, mechanisms or channels that will facilitate and allow for the transmission and execution of requests;

(d) have clear processes for the prioritisation and timely execution of requests; and

(e) have clear processes for safeguarding the information received.

40.3 Where competent authorities need bilateral or multilateral agreements or arrangements to cooperate, these should be negotiated and signed in a timely way, and with the widest range of foreign counterparts.

40.4 Upon request, requesting competent authorities should provide feedback in a timely manner to competent authorities from which they have received assistance, on the use and usefulness of the information obtained.

40.5 Countries should not prohibit, or place unreasonable or unduly restrictive conditions on, the provision of exchange of information or assistance. In particular, competent authorities should not refuse a request for assistance on the grounds that:

(a) the request is also considered to involve fiscal matters; and/or

(b) laws require financial institutions or DNFBPs (except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies) to maintain secrecy or confidentiality; and/or

(c) there is an inquiry, investigation or proceeding underway in the requested country, unless the assistance would impede that inquiry, investigation or proceeding; and/or

(d) the nature or status (civil, administrative, law enforcement, etc.) of the requesting counterpart authority is different from that of its foreign counterpart.

40.6 Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only for the purpose for, and by the authorities, for which the information was sought or provided, unless prior authorisation has been given by the requested competent authority.

40.7 Competent authorities should maintain appropriate confidentiality for any request for cooperation and the information exchanged, consistent with both parties' obligations concerning privacy and data protection. At a minimum, competent authorities should protect exchanged information in the same manner as they would protect similar information received from domestic sources. Competent authorities should be able to refuse to provide information if the requesting competent authority cannot protect the information effectively.

40.8 Competent authorities should be able to conduct inquiries on behalf of foreign counterparts, and exchange with their foreign counterparts all information that would be obtainable by them if such inquiries were being carried out domestically.

Exchange of Information between FIUs

40.9 FIUs should have an adequate legal basis for providing cooperation on money laundering, associated predicate offences and terrorist financing.

40.10 FIUs should provide feedback to their foreign counterparts, upon request and whenever possible, on the use of the information provided, as well as on the outcome of the analysis conducted, based on the information provided.

40.11 FIUs should have the power to exchange:

(a) all information required to be accessible or obtainable directly or indirectly by the FIU, in particular under Recommendation 29; and

(b) any other information which they have the power to obtain or access, directly or indirectly, at the domestic level, subject to the principle of reciprocity.

Exchange of information between financial supervisors

40.12 Financial supervisors should have a legal basis for providing cooperation with their foreign counterparts (regardless of their respective nature or status), consistent with the applicable international standards for supervision, in particular with respect to the exchange of supervisory information related to or relevant for AML/CFT purposes.

40.13 Financial supervisors should be able to exchange with foreign counterparts information domestically available to them, including information held by financial institutions, in a manner proportionate to their respective needs.

40.14 Financial supervisors should be able to exchange the following types of information when relevant for AML/CFT purposes, in particular with other supervisors that have a shared responsibility for financial institutions operating in the same group:

(a) regulatory information, such as information on the domestic regulatory system, and general information on the financial sectors;

(b) prudential information, in particular for Core Principles supervisors, such as information on the financial institution's business activities, beneficial ownership, management, and fit and properness; and

(c) AML/CFT information, such as internal AML/CFT procedures and policies of financial institutions, customer due diligence information, customer files, samples of accounts and transaction information.

40.15 Financial supervisors should be able to conduct inquiries on behalf of foreign counterparts, and, as appropriate, to authorise or facilitate the ability of foreign counterparts to conduct inquiries themselves in the country, in order to facilitate effective group supervision.

40.16 Financial supervisors should ensure that they have the prior authorisation of the requested financial supervisor for any dissemination of information exchanged, or use of that information for supervisory and non-supervisory purposes, unless the requesting financial supervisor is under a legal obligation to disclose or report the information. In such cases, at a minimum, the requesting financial supervisor should promptly inform the requested authority of this obligation.

Exchange of information between law enforcement authorities

40.17 Law enforcement authorities should be able to exchange domestically available information with foreign counterparts for intelligence or investigative purposes relating to money laundering, associated predicate offences or terrorist financing, including the identification and tracing of the proceeds and instrumentalities of crime.

40.19 Law enforcement authorities should be able to form joint investigative teams to conduct cooperative investigations, and, when necessary, establish bilateral or multilateral arrangements to enable such joint investigations.

Exchange of information between non-counterparts

40.20 Countries should permit their competent authorities to exchange information indirectly with non-counterparts, applying the relevant principles

above. Countries should ensure that the competent authority that requests information indirectly always makes it clear for what purpose and on whose behalf the request is made.

Annex 1 to the questionnaire for technical compliance update: size and structure of the financial and DNFBP sectors

AML/CFT Preventive Measures for Financial Institutions and DNFBPs (R.10 to R.23)

Type of Entity*	No. Licensed / Regulated / Registered	AML/CFT Laws** / Enforceable Means for Preventive Measures	Date in Force or Last Updated (*where applicable*)	Other additional Information (*e.g.* highlights of substantive changes etc.)***
Banks ХШҮГ	14	Yes		
Life Insurers СЗХ	1	Yes		
Securities СЗХ				
MVTS (money value transfer services) ХШҮГ, СЗХ				
Casinos	0			
Lawyers (өмгөөлөгч) BAR				
Notaries (нотариат) Н Танхим	215			
Accountants (мэргэшсэн нябо) МНБИ				
Precious Metals & Stones Dealers Татвар				
Trust and Company Service Providers Татвар				
Savings and credit cooperative СЗХ				
Non-banking Financial Institutions СЗХ				

*Additional rows may be added for other type of financial institutions and DNFBPs. Jurisdictions may also choose to have more granular and specific classification of the types of financial institutions and DNFBPs.

** Jurisdictions should indicate the specific provisions in the AML/CFT laws that set out the CDD, record keeping and STR reporting obligations.

***Where there have been changes since its last update or where relevant, jurisdictions should also set out the specific provisions in the AML/CFT laws or enforceable means and key highlights of the obligations for other preventive measures (*e.g.* PEPs, wire transfers, internal controls and foreign branches and subsidiaries etc.).

STATE REGISTRATION AND STATISTICS OFFICE OF MONGOLIA

Legal entity, type	Number of registered legal entities	Relevant law	Date got into force or last revised date
Shareholding company	295	**Company law**	**2011-10-06**
Limited liability company	103676	**Company law**	**2011-10-06**
State owned self- financing industrial organization	88	**Law about Government and local property**	**1996-05-27**
Local owned self-financing industrial organization	359	**Law about Government and local property**	**1996-05-27**
Government organization, office, state budget industrial	4318	**Law about Government and local property**	**1996-05-27**
Partnership	3609	**Law about partnership**	**1995-05-21**
Cooperative	3991	**Law about cooperative**	**1998-01-08**
Savings and credit cooperative	436	**Law about savings and credit cooperative**	**2011-10-27**
Non-profit organization	20862	**Law about Non-profit organization**	**1997-01-31**
Fund	979		
Mass media	3467		
Labour union organization	2531	**Law about labor unions**	**1991-04-19**
Religious organization	692	**Law about government, church, monastery relation**	**1993-11-11**
Foreign invested limited liability company	9187	**Law about investment** **Company law**	**2013-10-03** **2011-10-06**

Technical Compliance questionnaire Annex 1: FINANCIAL REGULATORY COMMITTEE

AML/CFT Preventive Measures for Financial Institutions and DNFBPs (R.10 to R.23)

Type of Entity*	No. Licensed / Regulated / Registered	AML/CFT Laws** / Enforceable Means for Preventive Measures	Date in Force or Last Updated (*where applicable*)	Other additional Information (*e.g.* highlights of substantive changes etc.)***
Insurance	17	Law on combating money laundering and	May 31, 2013,	

companies		terrorism financing, Regulation on prevention of money laundering and terrorist financing, know your customer, reporting of cash and suspicious transactions	November 22, 2009	
Life insurers	1	Law on combating money laundering and terrorism financing, Regulation on prevention of money laundering and terrorist financing, know your customer, reporting of cash and suspicious transactions	May 31, 2013,	
Securities	67	Law on combating money laundering and terrorism financing, Regulation on prevention of money laundering and terrorist financing, know your customer, reporting of cash and suspicious transactions	November 22, 2009	
Non-banking Financial Institutions	442	Law on combating money laundering and terrorism financing, Regulation on prevention of money laundering and terrorist financing, know your customer, reporting of cash and suspicious transactions	May 31, 2013,	
Money value transfer service	2			
Trust and Company Service Providers	18			
Credit Unions	254	Law on combating money laundering and terrorism financing	May 31, 2013,	
Others				

Registration of tax payers - By types of entity **GENERAL DEPARTMENT OF TAXATION, 2016/01/06**

Tax Authority	Share holdin	Limit ed	CAM L	SMH L	LL Coo	Coop erativ	Savings and	State own	Loc al	Branch es	Repre sentati	Budget organizat	NGO	Religiou s	Fun ds	Mass Media	Public organizatio	Double units	**TOTAL**

	g company	liability company			operative	e	credit cooperative	ed industrial organization	owned industrial organization		ve offices	ions		organizations			ns		
Arkhangai	7	530	17	60		221	4		2	54	1	196	144	14	10		1		1,261
Bayan-Ulgii	8	749	16	28	3	311	9	3	6	28		197	83	4	14		33		1,492
Bayankhongor	11	605	19	6	1	246	6	3	1	73		194	97	15	4	1	36		1,318
Bulgan	6	741	34	28		141	3		3	120		168	55	9	1		19		1,328
Gobi-Altai	4	463	17	12		123	3	3	13	92	1	200	80	2	5		5		1,023
Dornogobi	2	710	4	18		60	7	1	3	365		174	105	12	7		75		1,543
Dornod	12	1,104	39	15		80	6		15	168		151	129	7	5		38		1,769
Dundgobi	4	453	7			93	10	1	18	110		151	95	6	2		3		953
Zavkhan	3	797	41	20		374	24	1	8	95		232	163	15	7		25		1,805
Uvurkhangai	10	720	57	32		190	7	1	21	111		209	177	11	4		17		1,567
Umnugobi	5	1,300	16	29	1	87	8		36	357	5	182	142	4	13	1	16		2,202
Sukhbaatar	1	448	28	37		74	9	3	15	75		142	51	9	3		14	10	919
Selenge	15	1,568	187	48		160	3		14	401		219	131	21	32		25		2,824
Tuv	21	1,097	33	36		170	7	4	5	595		205	170	11	5		37		2,396
Uvs	15	1,027	19	8		210	5	1	7	81		189	112	7	2		12		1,695
Khovd	5	950	264	210	1	227	2	3	10	91	3	141	62	9	3		3		1,984
Khuvsugul	9	992	57	16		311	2	4	36	77		229	156	9	4		20	12	1,934
Khentii	9	840	11	35		128	7	2	9	173		198	113	9	4	4	36		1,578
Darkhan-Uul	22	2,432	53	139	1	111	8		9	209		115	321	38	4		116		3,578
Orkhon	7	3,048	40	116	2	58	14	1	7	145	2	100	304	24	9	14	71		3,962
General Department of Taxation	40	346			1		1	2				2							392
Capital city	23	1,364	2	1		1	2	19	29	132	47	77	305					1	2,003
Khan-Uul	12	8,905	72	57	13	52	29	12	8	578		139	964	24	94		172		11,131
Bayanzurkh	17	19,499	165	129	24	103	61	23	12	720		194	2,107	65	106		273		23,498
Sukhbaatar	12	17,172	145	113	44	102	92	23	7	643	5	331	2,291	40	136		401		21,557
Bayangol	28	19,730	179	129	15	82	98	8	6	1,234	6	159	1,668	43	83	2	318		23,788
Baganuur	2	398	12	12		10	7	3	2	60		39	121	6	3		5		680
Nalaikh	2	731	13	12		18	6	1	4	149		41	94	8	9		49		1,137

Gobisumber	1	220	4	9		17	1		5	62	2	55	48	5	6		14		449
Songinokhairhan	11	11,679	136	104	5	110	65	7	6	451	1	115	848	43	38	1	134		13,754
Chingeltei	10	11,433	120	88	33	54	67	29	7	731	8	256	1,415	39	87		193		14,570
TOTAL	**334**	**112,051**	**1,807**	**1,547**	**144**	**3,924**	**573**	**158**	**324**	**8,180**	**81**	**5,000**	**12,551**	**509**	**700**	**23**	**2,161**	**23**	**150,090**

Annex 2: STATE REGISTRATION AND STATISTICS OFFICE OF MONGOLIA

(2015/11/27)

Legal entities and regulation (RECOMMENDATIONS 8, 24, 25)

Legal entity, type	Number of registered legal entities	Relevant law	Date got into force or last revised date	Other additional Information **
Shareholding company	295	**Company law**	**2011-10-06**	
Limited liability company	103,676	**Company law**	**2011-10-06**	
State owned self- financing industrial organization	88	**Law about Government and local property**	**1996-05-27**	
Local owned self-financing industrial organization	359	**Law about Government and local property**	**1996-05-27**	
Government organization, office, state budget industrial	4,318	**Law about Government and local property**	**1996-05-27**	
Partnership	3,609	**Law about partnership**	**1995-05-21**	
Cooperative	3,991	**Law about cooperative**	**1998-01-08**	
Savings and credit cooperative	436	**Law about savings and credit cooperative**	**2011-10-27**	
NGO	20,862	**Law about Non-profit organization**	**1997-01-31**	
Fund	979			
Mass media	3,467			

Labour union organization	2,531	**Law about labor unions**	**1991-04-19**	
Religious organization	692	**Law about government, church, monastery relation**	**1993-11-11**	
Foreign invested limited liability company	9,187	**Law about investment** **Company law**	**2013-10-03** **2011-10-06**	
Shareholding company	295	**Company law**	**2011-10-06**	

*Additional rows may be added for other type of legal persons or arrangements. Jurisdictions may also choose to have more granular and specific classification of the types of legal persons or arrangements.

** Jurisdictions should indicate the specific provisions in the applicable laws / regulations / requirements and key highlights that set out the obligations to maintain the requisite information in R.24 (*e.g.* basic and beneficial ownership) and R.25 (*e.g.* settlers, trustees, protectors (if any), the (class of) beneficiaries, and any other natural person exercising control) respectively.

Annex 4

SURVEY ON EXECUTION DOCUMENTS WITH VALUE OF ABOVE 20 MILLION
/EXECUTION DEPARTMENT/

2015.12.04

Indications	Should be performed		Number of frozen assets		Number of confiscated assets					Number of assets resolved	
					Assets		Of which number of assets transferred for storage and safeguarding				
	Writ	Value	Movable	Immovable	Movable	Immovable	To execution unit	To payer	To third party	Sold	Transferred for payment
2010	1492	50 837 774,5	383	289	97	183	103	169	8	45	60
2011	1738	50 591 871,9	328	376	135	234	60	215	94	59	77
2012	2195	59 962 934,5	500	472	157	314	126	261	84	53	126
2013	2064	76 596 066,5	521	463	128	312	135	255	50	37	90

2014	1955	73 145 847,4	586	500	194	374	140	365	63	39	136
2015	2252	184 051 002,6	1585	718	890	492	802	476	104	46	798
Sum	11696	495 185 497,3	3903	2818	1601	1909	1366	1741	403	279	1287

EFFECTIVENESS ASSESSMENT

Immediate Outcome 1:

Money laundering and terrorist financing risks are understood and, where appropriate, actions co-ordinated domestically to combat money laundering and the financing of terrorism and proliferation.

1.1. How well does the country understand its ML/TF risks?

1.2. How well are the identified ML/TF risks addressed by national AML/CFT policies and activities.

1.3. To what extent are the results of the assessment(s) of risks properly used to justify exemptions and support the application of enhanced measures for higher risk scenarios, or simplified measures for lower risk scenarios?

1.4. To what extent are the objectives and activities of the competent authorities and SRBs consistent with the evolving national AML/CFT policies and with the ML/TF risks identified?

1.5. To what extent do the competent authorities and SRBs co-operate and co-ordinate the development and implementation of policies and activities to combat ML/TF and, where appropriate, the financing of proliferation of weapons of mass destruction?

1.6. To what extent does the country ensure that respective financial institutions, DNFBPs and other sectors affected by the application of the FATF Standards are aware of the relevant results of the national ML/TF risks?

EFFECTIVENESS ASSESSMENT

Immediate Outcome 2:

International co-operation delivers appropriate information, financial intelligence, and evidence, and facilitates action against criminal and their assets.

2.1. To what extent has the country provided constructive and timely mutual legal assistance and extradition across the range of international co-operation requests? What is the quality of such assistance provided?

2.2. To what extent has the country sought legal assistance for international co-operation in an appropriate and timely manner to pursue domestic ML, associated predicate offences and TF cases which have transnational elements?

2.3. To what extent do the different competent authorities seek other forms of international cooperation to exchange financial intelligence and supervisory, law enforcement or other information in an appropriate and timely manner with their foreign counterparts for AML/CFT purposes?

2.4. To what extent do the different competent authorities provide (including spontaneously) other forms of international co-operation to exchange financial intelligence and supervisory, law enforcement or other information in a constructive and timely manner with their foreign counterparts for AML/CFT purposes?

2.5. How well are the competent authorities providing and responding to foreign requests for co operation in identifying and exchanging basic and beneficial ownership information of legal persons and arrangements?

EFFECTIVENESS ASSESSMENT

Immediate Outcome 3:

Supervisors appropriately supervise, monitor and regulate financial institutions and DNFBPs for compliance with AML/CFT requirements commensurate with their risks.

3.1. How well does licensing, registration or other controls implemented by supervisors or other authorities prevent criminals and their associates from holding, or being the beneficial owner of a significant or controlling interest or holding a management function in financial institutions or DNFBPs? How well are breaches of such licensing or registration requirements detected?

3.2. How well do the supervisors identify and maintain an understanding of the ML/TF risks in the financial and other sectors as a whole, between different sectors and types of institution, and of individual institutions?

3.3. With a view to mitigating the risks, how well do supervisors, on a risk-sensitive basis, supervise or monitor the extent to which financial institutions and DNFBPs are complying with their AML/CFT requirements?

3.4. To what extent are remedial actions and/or effective, proportionate and dissuasive sanctions applied in practice?

3.5. To what extent are supervisors able to demonstrate that their actions have an effect on compliance by financial institutions and DNFBPs?

3.6. How well do the supervisors promote a clear understanding by financial institutions and DNFBPs of their AML/CFT obligations and ML/TF risks?

EFFECTIVENESS ASSESSMENT

Immediate Outcome 4:

Financial institutions and DNFBPs adequately apply AML/CFT preventive measures commensurate with their risks, and report suspicious transactions.

4.1. How well do financial institutions and DNFBPs understand their ML/TF risks and AML/CFT obligations?

4.2. How well do financial institutions and DNFBPs apply mitigating measures commensurate with their risks?

4.3. How well do financial institutions and DNFBPs apply the CDD and record-keeping measures (including beneficial ownership information and ongoing monitoring)? To what extent is business refused when CDD is incomplete?

4.4. How well do financial institutions and DNFBPs apply the enhanced or specific measures for: (a) PEPs, (b) correspondent banking, (c) new technologies, (d) wire transfers rules, (e) targeted financial sanctions relating to TF, and (f) higher-risk countries identified by the FATF?

4.5. To what extent do financial institutions and DNFBPs meet their reporting obligations on the suspected proceeds of crime and funds in support of terrorism? What are the practical measures to prevent tipping-off?

4.6. How well do financial institutions and DNFBPs apply internal controls and procedures (including at financial group level) to ensure compliance with AML/CFT requirements? To what extent are there legal or regulatory requirements (*e.g.*, financial secrecy) impeding its implementation?

EFFECTIVENESS ASSESSMENT

Immediate Outcome 5:

Legal persons and arrangements are prevented from misuse for money laundering or terrorist financing, and information on their beneficial ownership is available to competent authorities without impediments.

5.1. To what extent is the information on the creation and types of legal persons and arrangements in the country available publicly?

5.2. How well do the relevant competent authorities identify, assess and understand the vulnerabilities and the extent to which legal persons created in the country can be, or are being misused for ML/TF?

5.3. How well has the country implemented measures to prevent the misuse of legal persons and arrangements for ML/TF purposes?

5.4. To what extent can relevant competent authorities obtain adequate, accurate and current basic and beneficial ownership information on all types of legal persons created in the country, in a timely manner?

5.5. To what extent can relevant competent authorities obtain adequate, accurate and current beneficial ownership information on legal arrangements, in a timely manner?

5.6. To what extent are effective, proportionate and dissuasive sanctions applied against persons who do not comply with the information requirements?

EFFECTIVENESS ASSESSMENT

Immediate Outcome 6:

Financial intelligence and all other relevant information are appropriately used by competent authorities for money laundering and terrorist financing investigations.

6.1. To what extent are financial intelligence and other relevant information accessed and used in investigations to develop evidence and trace criminal proceeds related to ML, associated predicate offences and TF?

6.2. To what extent are the competent authorities receiving or requesting reports (e.g., STRs, reports on currency and bearer negotiable instruments) that contain relevant and accurate information that assists them to perform their duties?

6.3. To what extent is FIU analysis and dissemination supporting the operational needs of competent authorities?

6.4. To what extent do the FIU and other competent authorities co-operate and exchange information and financial intelligence? How securely do the FIU and competent authorities protect the confidentiality of the information they exchange or use?

EFFECTIVENESS ASSESSMENT

Immediate Outcome 7:

Money laundering offences and activities are investigated and offenders are prosecuted and subject to effective, proportionate and dissuasive sanctions.

7.1. How well, and in what circumstances are potential cases of ML identified and investigated (including through parallel financial investigations)?

7.2. To what extent are the types of ML activity being investigated and prosecuted consistent with the country's threats and risk profile and national AML/CFT policies?

7.3. To what extent are different types of ML cases prosecuted (*e.g.*, foreign predicate offence, third-party laundering, stand-alone offence etc.) and offenders convicted?

7.4. To what extent are the sanctions applied against natural or legal persons convicted of ML offences effective, proportionate and dissuasive?

7.5. To what extent do countries apply other criminal justice measures in cases where a ML investigation has been pursued but where it is not possible, for justifiable reasons, to secure a ML conviction? Such alternative measures should not diminish the importance of, or be a substitute for, prosecutions and convictions for ML offences.

EFFECTIVENESS ASSESSMENT

Immediate Outcome 8:

Proceeds and instrumentalities of crime are confiscated.

8.1. To what extent is confiscation of criminal proceeds, instrumentalities and property of equivalent value pursued as a policy objective?

8.2. How well are the competent authorities confiscating (including repatriation, sharing and restitution) the proceeds and instrumentalities of crime, and property of an equivalent value, involving domestic and foreign predicate offences and proceeds which have been moved to other countries?

8.3. To what extent is confiscation regarding falsely / not declared or disclosed cross-border movements of currency and bearer negotiable instruments being addressed and applied as an effective, proportionate and dissuasive sanction by border/custom or other relevant authorities?

8.4. How well do the confiscation results reflect the assessments(s) of ML/TF risks and national AML/CFT policies and priorities?

EFFECTIVENESS ASSESSMENT

Immediate Outcome 9:

Terrorist financing offences and activities are investigated and persons who finance terrorism are prosecuted and subject to effective, proportionate and dissuasive sanctions.

9.1. To what extent are the different types of TF activity (*e.g.*, collection, movement and use of funds) prosecuted and offenders convicted? Is this consistent with the country's TF risk profile?

9.2. How well are cases of TF identified, and investigated? To what extent do the investigations identify the specific role played by the terrorist financier?

9.3. To what extent is the investigation of TF integrated with, and used to support, national counter terrorism strategies and investigations (*e.g.*, identification and designation of terrorists, terrorist organisations and terrorist support networks)?

9.4. To what extent are the sanctions or measures applied against natural and legal persons convicted of TF offences effective, proportionate and dissuasive?

EFFECTIVENESS ASSESSMENT

Immediate Outcome 10:

Terrorists, terrorist organizations and terrorist financiers are prevented from raising, moving and using funds, and from abusing the NPO sector.

10.1. How well is the country implementing targeted financial sanctions pursuant to (i) UNSCR1267 and its successor resolutions, and (ii) UNSCR1373 (at the supra-national or national level, whether on the country's own motion or after examination, to give effect to the request of another country)?

10.2. To what extent, without disrupting legitimate NPO activities, has the country implemented a targeted approach, conducted outreach, and exercised oversight in dealing with NPOs that are at risk from the threat of terrorist abuse?

10.3. To what extent are terrorists, terrorist organisations and terrorist financiers deprived (whether through criminal, civil or administrative processes) of assets and instrumentalities related to TF activities?

10.4. To what extent are the above measures consistent with the overall TF risk profile?

EFFECTIVENESS ASSESSMENT

Immediate Outcome 11:

Persons and entities involved in the proliferation of weapons of mass destruction are prevented from raising, moving and using funds, consistent with the relevant UNSCRs.

11.1. How well is the country implementing, without delay, targeted financial sanctions concerning the UNSCRs relating to the combating of financing of proliferation?

11.2. To what extent are the funds or other assets of designated persons and entities (and those acting on their behalf or at their direction) identified and such persons and entities prevented from operating or executing financial transactions related to proliferation?

11.3. To what extent do financial institutions and DNFBPs comply with, and understand their obligations regarding targeted financial sanctions relating to financing of proliferation?

11.4. How well are relevant competent authorities monitoring and ensuring compliance by financial institutions and DNFBPs with their obligations regarding targeted financial sanctions relating to financing of proliferation?