Unofficial Translation

Important information:

This Sector Risk Assessment is intended to provide general and illustrative information to

1. assist banks to prepare and review their individual assessments of the risk of money laundering and the financing of terrorism under AML/CFT Law, and
2. inform and assist others involved in AML policy making and supervision in Mongolia and elsewhere.

The Sector Risk Assessment is not intended to cover all money laundering and terrorist financing risks that may be specific to the circumstances of individual banks.

The assessments and information in the Sector Risk Assessment relate solely to risks relating to money laundering and terrorism financing and do not reflect on the soundness of the sector, or individual banks.

Purpose of the SRA

This SRA undertaken by BoM in relation to the ML/TF risks in banking sector has the following purposes:

- It assists the AML/CFT supervisors in their understanding of particular ML/TF risks within banking sector;

- It provides guidance to banks on the risks relevant to their sector and informs their risk assessment;

- It contributes to the National risk assessment of ML/TF risks in Mongolia

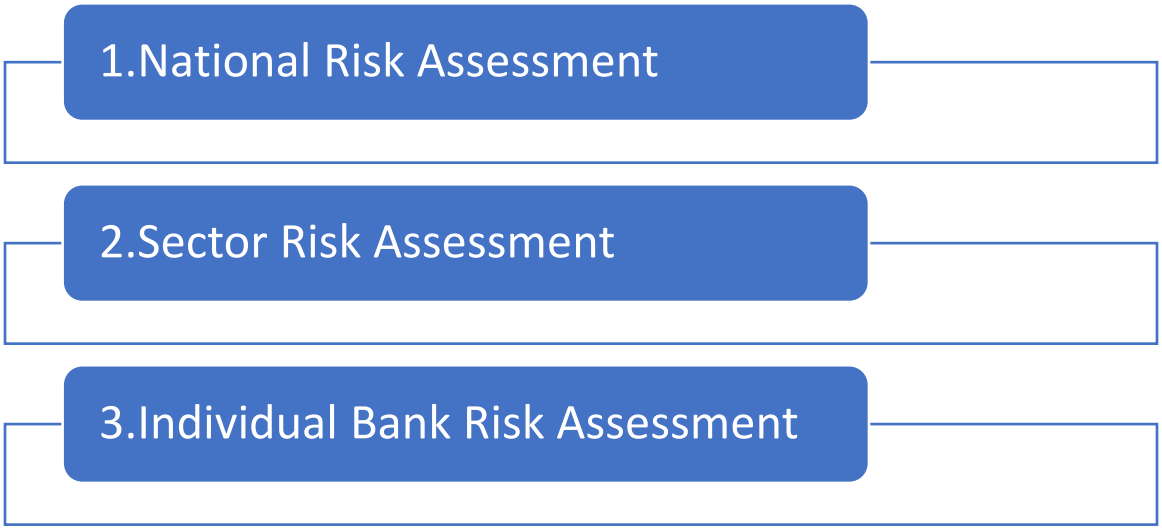
- It assists Mongolia in meeting FATF Recommendation 26 requiring countries to subject banks (and other financial institutions) to adequate AML/CFT regulation, licensing and supervision; and The SRA is also consistent with Basel Core principles (BCP8 - Supervisory approach and BCP 29 - Abuse of financial services) which states that supervisors should understand and monitor the risks to which the banking sector is exposed.

The risk-based approach (RBA) regime

The AML/CFT Law allows for a risk-based approach. In practice this means that banks should consider the potential vulnerabilities outlined in this document as part of their own risk assessments and consider whether these are priorities for their business to address and control. The purpose of a RBA is to minimize compliance costs and ensure that resources are targeted towards higher-risk, higher-priority areas. It is important to acknowledge that in a RBA regime reporting entities will not adopt identical AML/CFT policies, procedures or controls. Context is everything in regard to a RBA and no two reporting entities are exactly the same.

Three Levels of the risk assessment

Three levels of AML/CFT risk assessment are undertaken in Mongolia; national, sector and individual bank.
The following diagram outlines the inter-relationship of the risk assessment process:



National Risk Assessment (NRA) -The NRA gives an overview of ML/TF issues affecting Mongolia from a law enforcement perspective utilizing information from suspicious transaction reports (STRs) and proceeds of crime asset recovery data. Information from government organizations, both domestic and international, also contributes to this assessment. It is strongly recommended that banks refer to the NRA and the Typology reports in order to gain a better understanding of ML/TF risk.

Sector Risk Assessment (SRA) –The AML/CFT supervisors have each produced sector risk assessments. On-going SRA work will be conducted by

BoM in order to continually improve its understanding of the ML/FT risks associated with its sector and to inform banks of risk indicators, trends and emerging issues. The SRA may be revised regularly, or on an ad-hoc basis, depending on how ML/TF risks affect the banking sector.

Risk Assessments written by banks- Article 14 of the AML/CFT Law requires all reporting entities to undertake an assessment of the risk of ML/TF in their business. The risk assessment must consider the nature, size and complexity of its business, products and services (including delivery methods), customers and any countries and/ or institutions dealt with in the course of its business. One of the factors that reporting entities must have regard to when developing their risk assessments is guidance material produced by their AML/CFT Supervisor and the FIU. The SRA 2018 forms part of the AML/CFT guidance material issued by the BoM. Reporting entities are encouraged to access international AML/CFT guidance; the material produced by the FATF and the Asia Pacific Group on Money Laundering (APG).

Risk Appetite

Regardless of the assessed ML/TF risk and vulnerability ratings in the SRA 2018, when each reporting entity assesses its own ML/TF risk, consideration should be given to the level of risk it is willing to accept. A RBA recognizes that there can never be a zero ML/TF risk situation and each bank is expected to determine the level of AML/CFT control measures commensurate to the ML/TF risks to which it is exposed in order for those risks to be effectively mitigated. This is not a legislative requirement but may help banks with their risk management.

The AML/CFT Law facilitates co-operation amongst reporting entities, AML/CFT supervisors, and various government agencies, in particular law enforcement and regulatory agencies. BoM contributes to the administration of the AML/CFT regime by supervising compliance with the Law and monitoring and assessing levels of ML/TF risk banking sector that it supervises. The SRA 2018 is part of this.

ML activity has the potential to result in very serious social harm, criminal, financial and reputational consequences. Terrorism, while recognized as low risk within Mongolia, has the potential for catastrophic consequences.

Stages of Money Laundering

ML is generally considered to take place in three phases: placement, layering and integration. TF shares many of the characteristics of ML but may also involve legitimate funds and usually involve smaller amounts.

•**Placement**
occurs when criminals introduce proceeds of crime into the financial system. This might be done by breaking up large amounts of cash into less conspicuous

smaller sums that are then deposited directly into an account, or by purchasing shares or by loading credit cards. In some offences, such as fraud or tax evasion, placement is likely to occur electronically and may be inherent in the predicate offending.

•**Layering**

occurs once proceeds of crime are in the financial system. Layering involves a series of conversions or movements of funds to distance or disguise them from their criminal origin. The funds might be channeled through the purchase and sale of investment instruments or be wired through accounts at various banks across the globe. In some instances, the launderer might disguise the transfers as payments for goods or services, thus giving them a legitimate appearance.

•**Integration**

occurs once enough layers have been created to hide the criminal origin of the proceeds. This stage is the ultimate objective of laundering where funds re-enter the legitimate economy, such as in real estate, high value assets, or business ventures, allowing criminals to use the criminal proceeds of offending.

Nature and Size of the Banking sector

The role of banks in Mongolia's financial sector is significant with 14 local banks having a total 1482 branches and holding 20.8 trillion MNT (~8.6 billion USD) or 95.7% of total financial sector assets. Within the banking sector the three largest banks make up 70% or 14.56 trillion MNT (~6.04 billion USD) of total banking sector assets. There are no foreign banks conducting banking activities in Mongolia. Only one bank is 100% state owned and all other banks are privately owned. In addition, banks are gatekeepers for the non-bank sector and DNFPBs.

Banks may be used at all stages of ML/TF. Because of the wide availability and ease of accessibility of products and services the banking sector, as in most other countries, is considered a primary avenue for ML/TF. The value, volume and velocity of banking transactions provide an environment which conceals, disguises or obfuscates the proceeds of crime.

Products and services

Banks in Mongolia offer a wide range of products and services. In providing general banking facilities, banks offer a number of cash intensive products which have a high risk of being used to launder money. Proceeds from criminal activity have traditionally taken the form of physical currency at the placement stage of ML/TF. Placement of the proceeds of crime in the banking sector also occurs when criminal proceeds can be co-mingled with legitimate business takings before depositing into accounts.

Cash intensive products and services include quick-drop deposit facilities (e.g. Smart ATMs), over-the-counter services such as depositing or withdrawing cash,

sales and purchases of foreign exchange and purchase of pre-paid cash card products. Banks offer a wide range of products and services and it is beyond the remit of this assessment to list and assesses each of them. Banks should assess the ML/TF vulnerabilities associated with each of their products/services and consider:

- Are they highlighted by guidance as high risk?
- Do they support the physical movement of cash?
- Do they allow for international funds transfers?

Channels of delivery for products and services

Non-face-to-face application for, and delivery of, products/services is regarded as being more vulnerable to ML/TF activity than face-to-face delivery. Non face-to-face channels of delivery include internet banking, the use of intermediaries and the use of professional services/gatekeepers. Banks should assess the ML/TF vulnerabilities associated with the channels of delivery:

- Do they facilitate anonymity?
- Does the channel depend on intermediaries?
- Is the channel new or untested?

Customer types

Banks need to be aware of the ML/TF risks associated with customers. Banks should assess the ML/TF vulnerabilities associated with particular customer types. This can include certain occupations or industry links, whether they are individuals or legal persons, whether they are a Trust or if they have known criminal connections. Access to banking facilities by non-residents (see country risk- below) is also a factor that can increase the risk of ML/TF if there are no genuine reasons for operating an account in Mongolia.

The use of banking facilities by customers who are PEPs also heightens ML/TF risk due to their potential exposure to fraud, bribery and corruption. Likewise, high net worth customers pose a higher risk due to the larger amounts they have available to deposit or invest and the ease of fund movement through private banking type facilities. Banks in Mongolia offer services to all these types of customers. Also, of concern is the ability of non-customers using the banking system, for example by depositing cash into accounts held by other persons or companies, or one-off transactions such as currency exchange or wire transfers.

Country Risk

Country risk comes from dealing with persons, entities or countries in jurisdictions with poor or insufficient AML/CFT measures. Consideration should also be given to the levels of bribery and corruption, tax evasion, capital flight

and organized crime activity in a jurisdiction. In addition, a reporting entity should consider whether the country is a conflict zone and if the country is known for the presence of, or support of, terrorism.

Information on higher risk countries can be found from a number of information sources including the FATF, Transparency International, the United Nations Office on Drugs and Crime (UNODC), Basel AML index, and open source media. Banks will need to gain their own level of comfort when assessing country risk.

AML Compliance Officers will be expected to develop and maintain situational awareness around this topic and incorporate it into the AML/CFT Programme.

Institutions dealt with

Transaction accounts are maintained on a bank's behalf between domestic banks and between domestic banks and foreign banks. These accounts are used for international trade and investment, settlement, fund transfer facilities, the clearing of foreign items and to gain access to jurisdictions where a Mongolian bank has no physical presence.

International transactions have the potential to increase the risk of ML/TF occurring. Generally, banks international transactions flow through correspondent banking (Nostro and Vostro) accounts. A variety of activities are able to be accessed through correspondent banking accounts including nested and payable - through services. This may attract criminals to set up shell companies or banks abroad to engage in those activities. International cheque processing or bundling of money orders provide opportunities for launderers to pass off transactions as those of the originating bank thus bypassing monitoring similar to retail customer accounts.

Nested accounts or institutions offering payable through facilities provide further opportunities to disguise the underlying customer. Such relationships may serve to shield details of individuals through the pooled accounts at the financial institution level. The risk is reduced where overseas institutions have strong AML /CFT requirements, providing the underlying customer details are not shielded by a customer acting as a nominee.

Additional vulnerabilities or typologies

These specific vulnerabilities and typologies are provided as examples. Banks are expected to assess their own business specific vulnerabilities and to keep abreast of current guidance.

- Deposit quick drop facilities (including Smart ATMs)– The ease of use and anonymity afforded by these services are considered to present a high level of ML/TF risk for retail banks. This type of service has been highlighted both domestically and internationally as an area of concern. While BoM recognizes

that this service provides greater customer convenience and quicker deposit of funds the deposit of cash by unidentified persons remains a key vulnerability of this service.

- High value dealers– These customer types present a high ML/TF risk. Certain occupations and industries attract a higher risk rating for parts of the banking sector. These customer types include a broad spectrum of occupations and industries including real estate agents, cash intensive businesses, precious metal and stone dealers, car/motorbike dealers, jewelers.

Terrorism Financing (TF)

The terrorism threat that Mongolia itself faces is 'low'. Despite the low levels of TF risk, it is prudent for all banks to consider the potential vulnerabilities associated with TF and the potential red flags that may indicate TF activity.

TF funding covers a wide range of terrorism related activity including operational funds, equipment, salaries and family compensation, social services, propaganda, training, travel, recruitment and corruption. It is not necessary for reporting entities to identify the purpose of TF. Any potential TF related information must be reported to the FIU as soon as possible. Banks should consider not only high-risk countries but also their neighboring countries as TF often involves the movement of funds across borders. For instance, the UK NRA 2015 identifies Turkey, East Africa (especially areas surrounding Somalia) and the Persian Gulf as TF transit countries/regions.

Nature of TF

The characteristics of TF can make it difficult to identify. Transactions can be of low value, they may appear as normal patterns of behavior and funding can come from legitimate as well as illicit sources. However, the methods employed to monitor ML can also be applicable for TF as the movement of those funds often relies on similar methods to ML.

Internationally the TF process is considered to typically involve three stages:

- raising funds (through donations, legitimate wages, selling items or criminal activity);
- transferring funds (to a terrorist network, to a neighboring country for later pick up, to an organizational hub or cell); and
- utilizing funds (to purchase weapons or bomb-making equipment, for logistics, for compensation to families, for covering living expenses).

Given the global nature of TF and the constantly changing nature of international tensions and conflicts, the risks associated with TF are highly dynamic. As such, reporting entities need to ensure that their CFT measures are current, regularly reviewed and effective. It is important that reporting entities maintain situational awareness and effective transaction monitoring (TM) systems which incorporate dynamic TF risks as well as the more static risks associated with ML.

The value of funds moved through the international system in connection to TF is likely to be much lower than other forms of illicit fund flows. However, if funds connected to TF were to be associated with Mongolian financial institutions it would likely have a disproportionate effect on Mongolia's reputation rather than financial integrity. In addition, outside of the obvious harm caused by TF, any Mongolian bank associated with this activity would be subject to reputational repercussions and could be subject to potential civil and even criminal sanction.

The banking sector continues to be the most reliable and efficient way to move TF funds. TF through the banking sector can be small-scale and indistinguishable from legitimate transactions. TF could involve structured deposits of cash into bank accounts followed by wire transfers out of Mongolia. It could also involve banks being used by remittance agents to send funds overseas. NPO and charity accounts being used as fronts for sending funds offshore through the banking sector. Stored value cards (including credit cards) can be used to courier or access cash overseas, especially cards which enable withdrawals from international ATMs or allow multiple cards to be linked to common funds.

Given the difficulty with detecting TF, banks' TM systems and procedures (manual and electronic) play a key role in detecting TF activity. Furthermore, the banking sector's knowledge of their customers and their customer's expected financial transaction activity is vital in determining whether or not TF activity is potentially taking place.

Money Service Businesses (MSB)

MSBs are recognized internationally as presenting TF risk and banks should be aware of the risks associated with them. To some extent MSBs offer a degree of anonymity and an easy method of moving funds to countries that may have little or no formal banking structure, high levels of corruption and poor CFT measures. However, many communities and countries rely on the flow of funds using MSBs and AML/CFT responses to the risks presented by MSBs should be proportionate and reflect RBA.

Non-profit organizations (NPO) and charities

The use of NPOs and charities is an internationally recognized TF typology. NPOs can be used to disguise the movement of funds to high-risk regions and funds raised for overseas humanitarian aid can be co-mingled with funds raised for TF. NPOs can also easily and legitimately access materials, funds and networks of value to terrorist groups. In addition, funds sent overseas by charities with legitimate intentions can also be intercepted when they reach their destination country.

The FATF report that NPOs most at risk of abuse are those engaged in ‘service’ activities which are operating in close proximity to an active terrorist threat. Funds sent to high risk jurisdictions for humanitarian aid are at increased risk of being used for TF if they are sent through less established or start-up charities and NPOs.
Some donors may willingly provide donations to support terrorist groups, while other donors, and the charities themselves, may be coerced, extorted or misled about the purpose of funding. However, it is important to consider this TF vulnerability in the context of the Mongolian environment and that this will not apply to the vast majority of Mongolian charities and NPOs.

Cash couriers
TF risk associated with cash couriers is assessed internationally as high. This method of TF may be undertaken by multiple individuals and involve smuggling cash across porous borders to high risk TF jurisdictions. Bulk cash smuggling can also be utilized.
.

TF indicators and warnings (I&W)

ML and TF share many I&W or red flags. The following I&W may assist reporting entities in the difficult task of drawing a link between unusual or suspicious activity and TF. The list is not exhaustive and banks are encouraged to identify I&W which may occur in their course of business as part of their risk assessment. Red flags which may occur within the banking sector include:
- Structured cash deposits and withdrawals, potentially at multiple branches of the same reporting entity;
- Multiple customers and/or occasional transactions by non customers conducting transactions to the same beneficiary located in a high-risk jurisdiction;
- A customer conducting fund transfers to multiple beneficiaries located in high-risk jurisdictions;
- A customer using incorrect spelling or providing variations on their name when conducting funds transfers to high-risk jurisdictions;
- Transfer of funds between business accounts and personal accounts inconsistent with the type of account held and/or the expected transaction volume for the business;
- Large cash deposits and withdrawals to and from NPO accounts;
- Individuals and/or businesses transferring funds to listed terrorist entities or entities reported in the media as having links to terrorism or TF;
- Multiple low-value domestic transfers to a single account and cash deposits made by multiple third parties;
- A sudden increase in account activity, inconsistent with customer profile;
- Multiple cash deposits into personal account described as ‘donations’ or ‘contributions to humanitarian aid’ or similar terms;
- Transfers through multiple accounts followed by large cash withdrawals or outgoing fund transfers overseas;

- Multiple customers using the same address/telephone number to conduct account activity;
- Proscribed entities or entities suspected of terrorism using third-party accounts (for example, a child's account or a family member's account) to conduct transfers, deposits or withdrawals;
- Use of false identification to establish Mongolian companies;
- Pre-loading credit cards, requesting multiple cards linked to common funds or demanding multiple stored value cards prior to travel in order to courier cash overseas;
- Customers taking out loans and overdrafts with no intention or ability to repay them or using fraudulent documents;
- Customers emptying out bank accounts and savings;
- Customers based in or returning from conflict zones;

Over all risk rating of banking sector is High

The overall High-risk rating for banks is consistent with the characteristics of the banking industry in the absence of AML/CFT controls. This is to be expected given the relative size of the banking sector, the large number of customers and the high number and value of transactions compared to other FIs. Combined with The wide availability and easy accessibility of products and services and access to international financial systems the banking sector presents a much greater risk of ML/TF than the other sectors.

Methodology- Assessment of risk

ML/TF risk for banking sector was assessed using the variables contained in Article 14.4.1 of the AML/CFT Law and Regulation of off-site supervision of the banks on anti-money laundering and combating financing of terrorism and proliferation. these variables include the nature, size, structure and its products/services, the channels it uses for delivery of products/services, its customer types, and the countries and institutions that it deals with. Assessing risk by these variables was done to help reporting entities use the SRA 2018 in their own ML/TF risk assessments.

For each of these variables several ML/TF factors were considered and helped guide the assessment of inherent ML/TF risk associated with each variable. This was done in combination with professional opinion, domestic and international guidance and the findings of the BoM's Entity/Bank Risk Assessment (ERA). At the end of this process an overall assessment of inherent
ML/TF risk was then rated as Low, Medium or High.

BoM decided not to consider the adequacy or effectiveness of ML/TF controls in the risk rating process and no judgements were formed on whether the risks present in banking-sector were effectively managed or mitigated. Banks may

have systems and controls that address some or all of the risks discussed in the risk assessment but the SRA 2018 does not identify or comment on activities undertaken by individual banks.

The absence of an assessment of residual risk was a deliberate course of action designed to simplify the SRA process. Banks, as part of their AML/CFT Programme, are expected to address the inherent risks identified in their Risk Assessment.

Methodology – Identification of vulnerabilities

As part of the SRA 2018, 12 key ML/TF vulnerabilities were identified. The vulnerabilities were identified and selected during a series of BoM, GIA, GPA and FIU workshops based on subject matter expertise, supervision experience gained during onsite visits, and domestic and international guidance. The vulnerabilities were chosen for their commonality across banking sector and were kept few to assist reporting entities to understand the most significant ML/TF vulnerabilities in Mongolia.

Predicate offending and STRs

It is important for reporting entities to understand the offending and criminal behavior which leads to ML/TF. This is called predicate offending. However, reporting entities are not required to prove the predicate offence when investigating or reporting STRs. NRA identified most common predicate offences and threats.

Tax evasion – The NRA identified tax evasion as a significant proceeds of crime generator, and recent media reports support this conclusion.

Environmental crimes– The NRA identifies environmental crimes as a significant proceeds of crime generator.

Corruption and bribery– The NRA identified corruption as a significant proceeds of crime generator. Mongolia's Transparency International corruption perception index supports this conclusion. In addition, a number of Mongolian politically exposed persons (PEPs) were named in the International Consortium of Investigative Journalists investigation into offshore companies.

Fraud – The NRA identifies fraud as a significant proceeds of crime generator.

ML/TF Vulnerabilities

Vulnerability	Comment
Gatekeepers	Professional 'gatekeepers' such as lawyers, accountants, foreign trust and company service providers (TCSPs) and real estate agents have long been identified as a ML/TF vulnerability. In addition, the consequences if professional services are being abused by ML/TF have the potential to be high. • DNFBPs newly covered in the AML/CFT Law and are particularly vulnerable to ML/TF abuse. • The involvement of a professional gatekeeper can provide launderers with the impression of respectability, legitimacy and/or normality especially in large transactions. It also provides a further step in the laundering chain which frustrates detection and investigation. • Professionals may also allow launderers to access services and techniques that they would not ordinarily have access to. This may be as simple as making introductions (e.g. to open an account) • Vulnerabilities in the legal profession (which also apply to accountants) include the use of client accounts, purchase of real estate (this would also apply to other purchases of large assets and businesses), and managing client affairs. While each of these areas are legitimate services these services may be exploited by money launderers and/or terrorist financiers. • The use of intermediaries, such as brokers, present a number of ML/TF vulnerabilities. The increased risk stems from the ability of intermediaries to control the arrangement and the sales environment in which they may operate. •Use of intermediaries may also circumvent some of the due diligence effectiveness by obscuring the source of the funds from third parties. For some reporting entities, the use of intermediaries may be their sole distribution channel and for others it may account for an increasing market share leaving them open to ML/TF risk. • NRA also reports on the attractiveness of the real estate sector to money launderers. The
Trusts and shell companies	
International payments	
Cash	
International trade and trade-based ML	
New payment technology	
Cards	
Anonymity	
High risk customers	
High risk jurisdictions	
Money Service Business	
ML/TF awareness	

	value of the sector, the volume of sales and the low level of detection capacity make the real estate sector highly vulnerable to layering and integration of criminal proceeds.