SECTORAL RISK ASSESSMENT

On Money Laundering And Terrorism Financing

Non-Bank Payment System Service Providers
And Money Changers

Governor's Foreword

All Praise be to the Lord God Almighty for His blessings and guidance bestowed upon us to accomplish this Sectoral Risk Assessment on Money Laundering and Terrorism Financing for Non-Bank Payment Service Providers and Money Changers.

Money laundering and terrorism financing represent a grave threat to economic stability and the integrity of the financial system, while endangering the very fabric of society, the state, and the country. Bank Indonesia is fully committed to support policies adopted by the Government of the Republic of Indonesia in preventing money laundering and combating the financing of terrorism, through the roles of Bank Indonesia as the payment system authority.

Under the Anti-Money Laundering and Combating the Financing of Terrorism regime, Financial Institutions not only help to bolster law enforcement but also simultaneously shield themselves from being exploited as a means and target for money laundering and terrorism financing. In this regard, sectoral risk assessments play an important role so that Financial Institutions will be able to understand, identify, and measure the risks of money laundering and terrorism financing focusing on four risk factors, namely customer risk, regional risk, product/service risk, and delivery channel risk. In this context, Bank Indonesia has enacted regulations and adopted policies, granted and revoked licenses, undertaken supervision, and imposed sanctions on Non-Bank Payment Service Providers and Non-Bank Money Changers that fall under the jurisdiction of Bank Indonesia, in accordance with prevailing laws.

Against this backdrop, I warmly welcome the publication of the Sectoral Risk Assessment on Money Laundering and Terrorism Financing for Non-Bank Payment System Service Providers and Money Changers. Through this risk assessment, the potential risks on money laundering and terrorism financing crimes can be mapped and mitigated, so as to support the integrity of the financial system, increase the credibility and reputation of Indonesia, and in accordance with the international standards including the recommendations of the Financial Action Task Force (FATF).

May the Lord God Almighty always bless and guide us.

Governor of Bank Indonesia

Perry Warjiyo

CONTENTS

LIST OF TABLES

LIST OF FIGURES

PART 1

1 INTRODUCTION

A. Background

Money laundering (ML) and terrorism financing (TF) represent extraordinary offences that can threaten economic stability and financial system integrity and can endanger the fabric of society, the state and the country. In accordance with the first recommendation of the Financial Action Task Force (FATF), each country is required identify, analyse and evaluate the money laundering (ML) and terrorism financing (TF) risks that they are exposed to. Such countries are then expected to take action, determine which authorities will coordinate the risk assessment and utilise data sources to ensure that the risks are effectively mitigated. In Indonesia, this was achieved by issuing laws and appointing Supervisory and Regulatory Bodies (LPP) along with designating their tasks and function.

Indonesia has comprehensively updated its identification, analysis and evaluation processes for various money laundering and terrorism financing risks through a National Risk Assessment (NRA), namely NRA 2015 Updated. NRA 2015 Updated provides various information concerning domestic and international money laundering and terrorism financing risks from 2015-2018, the latest potential threats, anti-money laundering and counter-terrorism financing strategies, as well as policies to implement as a follow-up to the NRA. To that end, Indonesia has compiled a National Strategy for the Prevention and Eradication of Money Laundering and Terrorism Financing (Stranas).

One of the Action Plans contained in Stranas is a Sectoral Risk Assessment (SRA) in Indonesia. The SRA is compiled by the respective LPP and law enforcement apparatus (Apgakum) for each sector under their authority. SRA is expected to provide a comprehensive illustration of sectoral risks as well as information on the key risks, trends and modi operandi of ML and TF in each sector.

Under the regime in Indonesia to prevent and eradicate ML and TF, in accordance with prevailing laws, Bank Indonesia will act as LPP to Payment System Service Providers (PJSP) and Non-Bank Money Changers (KUPVA BB). As the LPP, Bank Indonesia is tasked with maintaining the payment system industry, including KUPVA BB, in order to avoid the payment system being exploited or targeted for ML and TF. As a preliminary risk mitigation measure, Bank Indonesia, in conjunction with the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC), has assessed and updated the ML and TF risks in the SRA based on services users, geographic location, products/services and delivery channels, which will be used as a foundation to set the supervision priorities as well as allocate resources for ML and TF prevention.

B. Objectives

The objectives of the risk assessment in the PJSP and KUPVA BB sector are as follows:

1. To identify and analyse the ML and TF threat, including cases of ML and TF as well as the Suspicious Financial Transaction Report (STR)[1];

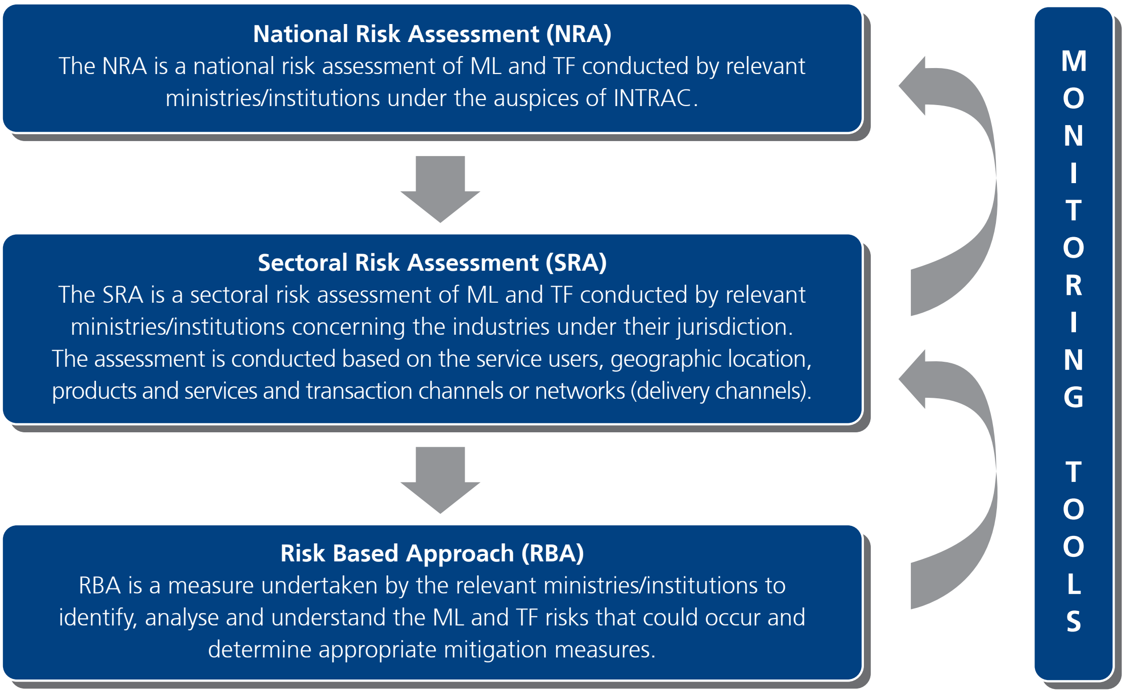
[1] The Suspicious Financial Transaction Report (STR) is submitted to the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC) detailing suspicious financial transactions initiated by service users.

2. To identify vulnerabilities and the consequences of money laundering and terrorism financing; and
3. To analyse the key risks of money laundering and terrorism financing, which involves mapping the risks in terms of the **service users, geographic locations, products and transaction channels or networks (delivery channels).**

C. Outcomes

SRA is expected to form a solid policymaking foundation for Bank Indonesia and the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC), particularly in relation to regulations and supervision of Anti-Money Laundering and Countering Terrorism Financing (AML/CFT) in the PJSP and KUPVA BB sector. In addition, the results of the SRA are also expected to provide sound guidelines for PJSP and Non-Bank Money Changers in the identification of business risks relating to their operating activities as well as appropriate preventative measures. The following flowchart illustrates the risk assessment process (Figure 1.1.1):

Figure 1.1.1.
Risk Assessment Process



National Risk Assessment (NRA)
The NRA is a national risk assessment of ML and TF conducted by relevant ministries/institutions under the auspices of INTRAC.

Sectoral Risk Assessment (SRA)
The SRA is a sectoral risk assessment of ML and TF conducted by relevant ministries/institutions concerning the industries under their jurisdiction. The assessment is conducted based on the service users, geographic location, products and services and transaction channels or networks (delivery channels).

Risk Based Approach (RBA)
RBA is a measure undertaken by the relevant ministries/institutions to identify, analyse and understand the ML and TF risks that could occur and determine appropriate mitigation measures.

2 AML/CFT REGIME

A. The AML/CFT Regime in Indonesia

The rapid development of technology, communications and information is increasing the complexity and diversity of financial transactions. This could potentially amplify ML and TF risks, for instance in terms of the modi operandi and typology. Currently, ML and TF not only exploit institutions in the financial system yet also exploit various non-financial sectors. In anticipation, FATF has issued international standards as a reference for each country in the prevention and eradication of money laundering and terrorism financing, which are known collectively as the FATF 40 Recommendations[2].

The handling of ML in Indonesia was strengthened with the enactment of Act No. 15 of 2002, which was subsequently amended by Act No. 25 of 2003 and Act No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering (AML Act). In addition, the eradication of TF in Indonesia was strengthened by Act No. 9 of 2013 on the Prevention and Eradication of Terrorism Financing (CFT Act). Through those laws, Indonesia has:

1. Adjusted to the needs of international practices and standards; and
2. Provided legal assurance for effective law enforcement, including provisions to search and recover proceeds of crime.
3. In addition, the prevailing laws are expected to garner public confidence in Indonesia by maintaining financial system integrity.

In the fight to prevent and eradicate ML and TF, Bank Indonesia collaborates with various stakeholders as follows:

1. **National Committee on ML Prevention and Eradication (Komite TPPU)**

   Based on Presidential Regulation No.117 of 2016, as an amendment to Presidential Regulation No. 6 of 2012 concerning the National Committee on ML Prevention and Eradication, the Komite TPPU was established to increase effective coordination between institutions in the prevention and eradication of money laundering. The Komite TPPU also serves the following functions:

   a. Formulate the direction, policies and strategy for ML prevention and eradication;
   b. Coordinate program and activity implementation in accordance with the direction, policies and strategy for ML prevention and eradication;
   c. Coordinate the measures necessary to handle other aspects relating to the prevention and eradication of ML, including TF; and
   d. Monitor and evaluate the handling as well as program and activity implementation in accordance with the direction, policies and strategy for ML prevention and eradication.

[2] The FATF 40 Recommendations are standards issued by FATF, providing a complete set of countermeasures against money laundering and terrorism financing through laws, financial system regulations and international cooperation. The FATF 40 Recommendations are accessible from https://www.fatf-gafi.org/publications/fatfrecommendations/documents/the40recommendationspublishedoctober2004.html.

The Komite TPPU consists of the following members:

Chairman :
Coordinating Minister for Political, Legal and Security Affairs

Vice Chairman :
Coordinating Minister for Economic Affairs

Secretary :
Head of the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC)

Members :

1. Minister of Foreign Affairs
2. Minister of Domestic Affairs;
3. Minister of Finance;
4. Minister of Law and Human Rights;
5. Minister of Trade;
6. Minister of Cooperatives and Small and Medium Enterprises;
7. Governor of Bank Indonesia;
8. Chairman of the OJK Board of Commissioners;
9. Attorney General;
10. Chief of National Police of Indonesia;
11. Chief of the State Intelligence Agency;
12. Chief of the National Agency for Combating Terrorism; and
13. Head of the National Anti-Narcotics Agency

Implementation Team :

Chairman :
Head of the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC)

Vice Chairman :
Deputy Coordinating Minister for Security and Public Order

Member :

1. Deputy Coordinating Minister for Law and Human Rights;
2. Deputy Coordinating Minister for International Economic Cooperation;
3. Deputy Governor of Bank Indonesia for the Payment System;
4. Head of the Commodity Futures Trading Supervisory Agency, Ministry of Trade;
5. Deputy for Financing of the Ministry of Cooperatives and Small and Medium Enterprises;
6. Deputy for Supervision of the Ministry of Cooperatives and Small and Medium Enterprises;
7. Chief Executive of Banking Supervision, Financial Services Authority;
8. Director General of Customs and Excise, Ministry of Finance;
9. Director General of Tax, Ministry of Finance;
10. Director General of State Assets, Ministry of Finance;
11. The Secretary General of Ministry of Finance;
12. Director General for Multilateral Cooperation, Ministry of Foreign Affairs;
13. Director General of International Law and Agreements; Ministry of Foreign Affairs;
14. Director General of General Legal Administration, Ministry of Law and Human Rights;
15. Director General of Immigration, Ministry of Law and Human Rights;
16. Director General of National Unity and Political Affairs; Ministry of Home Affairs;
17. Director General of Population and Civil Registration, Ministry of Home Affairs;
18. Deputy Attorney General for General Crime;
19. Deputy Attorney General for Specific Crime;
20. Chief of the Criminal Investigation Agency;
21. Chief of Special Detachment 88 Anti-Terror;
22. Deputy of Counterintelligence;
23. Deputy for Enforcement and Capacity Building of the National Agency for Combating Terrorism; and
24. Deputy of Eradication, National Anti-Narcotics Agency;

In an effort to coordinate and ensure the effectiveness of efforts to prevent and eradicate ML and TF, the Komite TPPU has compiled National Strategy (Stranas). Stranas may be used as a reference for ministries/institutions/organisations incorporated under the auspices of the ML Committee as well as other relevant parties when compiling programs or implementing activities in accordance with the direction, policies and strategy for ML prevention and eradication.

2. Reporting Party

Pursuant to Article 1 of the AML Act, a Reporting Party means any person required to submit a report to INTRAC in accordance with prevailing laws. INTRAC has already expanded the scope of Reporting Parties as stipulated in Article 17, paragraph (1) of Act No.8 of 2010 concerning AML Act as well as Article 2 and Article 3 of Government Regulation No.43 of 2015 concerning the Reporting Parties in the Prevention of Money Laundering. A reporting party includes:

a. Financial Service Providers (PJK):
   1) Banks;
   2) Finance companies;
   3) Insurance companies and brokers;
   4) Pension funds;
   5) Securities companies;
   6) Investment managers;
   7) Custodian banks;
   8) Trustees;
   9) Current account service providers;
   10) Foreign exchange traders;
   11) Card-based payment instrument issuers;
   12) e-money and or e-wallet issuers;
   13) Savings and loans cooperatives;
   14) Pawnbrokers;
   15) Commodity futures traders;
   16) Remitters/money transfer services providers;
   17) Venture capital firms;
   18) Infrastructure financing companies;
   19) Microfinance institutions; and
   20) Export financing companies.

b. Providers of Other Goods and/or Services (PBJ):
   1) Property companies/agents;
   2) Motor vehicle traders;
   3) Traders of jewellery and gems/precious metals;
   4) Traders of artwork and antique goods; and
   5) Auctioneers.

c. Professional Services:
   1) Advocate;
   2) Notary;
   3) Land deeds;
   4) Accountants;
   5) Public accountants; and
   6) Financial planners.

3. Supervisory and Regulatory Bodies (LPP)

Article 1, paragraph 17 of the AML Act states that Supervisory and Regulatory Bodies (LPP) are institutions with the authority to supervise, regulate and/or impose sanctions on a Reporting Party. Therefore, LPP in Indonesia include Bank Indonesia, the Financial Services Authority (OJK), Indonesian Financial Transaction Reports and Analysis Centre (INTRAC), Ministry of Cooperatives, Ministry of Trade and Ministry of Finance.

4. Public

The public plays a critical role in the prevention and eradication of ML and TF. Under an anti-money laundering and counter-terrorism financing regime, the public can play an active role in terms of providing information concerning ML and TF to INTRAC, Law Enforcement Apparatus and other relevant parties.

B. AML/CFT Regime in Bank Indonesia

Striving to prevent and eradicate ML and TF, Bank Indonesia applies three salient strategies as follows:

1. Complying with national and international AML/CFT standards or principles;
2. Building public and industry awareness concerning the ML and TF risks; and
3. Increasing national and international coordination/cooperation amongst institutions.

1. **Complying with national and international AML/CFT standards or principles**

   From a regulatory perspective, Bank Indonesia has issued Bank Indonesia Regulation (PBI) No. 19/10/PBI/2017 concerning the Implementation of Anti-Money Laundering and Countering Terrorism Financing for Payment System Service Providers and Money Changers (PBI AML/CFT). The provisions contained in PBI AML/CFT became effective in September 2017, targeting non-bank payment system service providers, namely money transfer services providers, card-based payment instrument issuers, e-money and e-wallet issuers as well as money changers.

   The Bank Indonesia Regulation also stipulates the AML/CFT requirements specific to payment system service providers[3] and money changers as follows:

   a. tasks and responsibilities of the directors and active supervision of the Board of Commissioners;
   b. policies and written procedures;
   c. risk-management processes;
   d. human resources management; and
   e. internal control system.

   In terms of supervision, Bank Indonesia applies risk-based supervision of AML/CFT implementation as a continuous activity of identifying, monitoring and assessing the risks. In the application of a Risk-Based Approach, Bank Indonesia has already compiled RBA guidelines referring to the SRA as a guide for supervisors and service providers in the identification, assessment an understanding of ML and TF risks.

2. **Building Public and Industry Awareness concerning the ML and TF Risks**

   Striving to build public and industry awareness concerning the ML and TF risks, Bank Indonesia is actively providing educational activities and a public campaign. For example, Bank Indonesia has urged the public to use authorised payment system service providers and money changers. Furthermore, Bank Indonesia has instructed service providers to reject transactions initiated without identification, to detect suspicious financial transactions and report such transactions to INTRAC. Education has been provided through various channels, including print media, social media and direct meetings with service providers and the public.

3. **Increasing Inter-Institutional Cooperation**

   To prevent the payment system from being exploited to facilitate ML and TF, Bank Indonesia has also cooperated and coordinated intensively with other relevant authorities, including INTRAC, National Police of the Republic of Indonesia, National Anti-Narcotics Agency (BNN), Corruption Eradication Commission (KPK) and Financial Services Authority (OJK). In addition, Bank Indonesia is also cooperating with central banks of other countries i.e. Bangko Sentral Ng Pilipinas and Bank of Thailand

C. Development of New Technology and Technology-Based Service Providers

Referring to Stranas and in response to the rapid development of new technology, Bank Indonesia issued Bank Indonesia Regulation (PBI) No. 19/12/PBI/2017 concerning Financial Technology (FinTech) Companies. The Bank Indonesia regulation states that FinTech companies, which are considered payment system service providers, must obtain a licence from Bank Indonesia in accordance with prevailing Bank Indonesia regulations concerning payment transaction processing. Consequently,

[3] Non-Bank payment system service providers subject to the PBI AML/CFT include money transfer service providers, card-based payment instrument issuers as well as e-money and e-wallet issuers.

Non-Bank FinTech companies already licensed by Bank Indonesia are required to comply with the PBI AML/CFT, while paying due attention to the SRA in relation to the business operating licence held. To issue e-money, for example, a Non-Bank FinTech company is required to hold a licence to issue e-money, comply with the PBI AML/CFT and refer to the SRA on e-money.

The e-wallet sector is not subject to a separate SRA. An e-wallet entails electronic services to store payment instrument data, such as card-based payment instruments and/or e-money, which may also be used to initiate payments[4]. In practice, authorised non-bank e-wallet issuers are also e-money issuers that provide additional services for non-cash payment instruments issued by a separate issuer. Therefore, the SRA for e-Money Issuers in Indonesia also contains an assessment of AML/CFT implementation for e-Wallet Issuers in Indonesia.

The Currency Act (No. 7) of 2011 stipulates that currency is issued by the Republic of Indonesia, known as the Rupiah. In reference to that law, Bank Indonesia has reiterated that virtual currency is not recognised as legal tender and, therefore, prohibited as a payment instrument in Indonesia[5]. Bank Indonesia has also proscribed payment system service providers from receiving, using and/or processing payment transactions using virtual currency in accordance with PBI PTP[6], PBI FinTech[7] and PBI E-Money[8].

D. NRA ML and TF for 2015 Updated

Striving to prevent and eradicate ML and TF, one instrument that can be used to ensure effective implementation is the NRA. Through the NRA, the stakeholders are able to understand the ML and TF risks based on their exposure. Overhauling ML and TF in Indonesia, the Indonesian Government, under the auspices of the Komite TPPU, updated the 2015 NRA. In 2019, Indonesia issued NRA 2015 Updated, which identified the current risks and mitigation measures undertaken by Indonesia from 2015-2018.

Based on the risk identification and mitigation plan initiated in Indonesia, the NRA recommends priority actions. Priority actions cover prevention by strengthening RBA implementation and domestic coordination along with formal and informal international cooperation.

[4] Article 1, paragraph 7 of Bank Indonesia Regulation (PBI) No. 18/40/PBI/2016 concerning Payment Transaction Processing.

[5] The announcement was made through Press Release No.20/4/DKom, dated 13th January 2018, entitled 'Bank Indonesia Warns All Parties not to Sell, Buy or Trade Virtual Currency'.

[6] Bank Indonesia Regulation (PBI) No.18/40/PBI/2016 concerning Payment Transaction Processing.

[7] Bank Indonesia Regulation (PBI) No.19/12/PBI/2017 concerning Financial Technology.

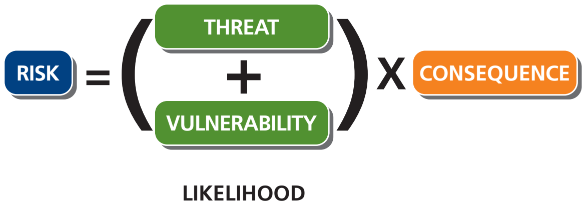
[8] Bank Indonesia Regulation (PBI) No.20/6/PBI/2018 concerning E-Money.

3 SECTORAL RISK ASSESSMENT METHODOLOGY

A. Framework

The framework used to prepare the Sectoral Risk Assessment refers to the FATF standard guidelines on National Money Laundering and Terrorism Financing Risk Assessment, as general guidelines, with the risk factors including threats, vulnerabilities and consequences (Figure 1.3.1).

Figure 1.3.1.
Risk Assessment Framework



Risk is a function of threat, vulnerability and consequence. A threat constitutes a person or group of persons, object or activity that poses a potential threat to the state, social fabric or economy. In the context of ML and TF, a threat includes perpetrators of crime, criminal organisations, other relevant parties, proceeds of crime and so on. A vulnerability is something that can be exploited by a threat to commit an offence. In the context of ML and TF, vulnerability exposes a weakness in the anti-money laundering and counter-terrorism financing regime on the reporting side. A consequence is the impact that arises in an anti-money laundering and counter-terrorism financing regime to the financial system, financial industry, economy or social fabric in general.

Based on the FATF guidelines, the risk assessment consists of three stages as follows:

1. **Identification.** Identifying the threats and vulnerabilities as well as the consequences. Ideally, the identification process is rigorous and comprehensive, yet may also be dynamic, implying that new and previously identified risks should also be considered at each stage.

   Risk identification in non-bank payment system service providers and money changers will produce four key risks as the focus for efforts to prevent and eradicate ML and TF, including:

   - Customer Profile
   - Products and Services
   - Location
   - Delivery Channel

   The risk factor matrix to identify threats, vulnerabilities and consequences used in the risk assessment is as follows (Table 1.3.1):

Table 1.3.1.
Risk Factor Matrix applicable to Non-Bank Payment System Service Providers and Money Changers

Non-Bank Payment System Service Providers and Money Changers
THREAT
Threat Factor Assessment
• Suspicious Transaction Reports (LKTM)
• Total high-risk customers
• Total product and service users
• Total customer services offices

Non-Bank Payment System Service Providers and Money Changers

VULNERABILITY

Vulnerability Factor Assessment

- Tasks and responsibilities of the directors and active supervision of the board of commissioners
- Adequate policies and written procedures
- Effective risk-management
- Adequate HR management
- Internal control system based on professional judgement
- Ability to identify and report suspicious financial transactions relating to the customer profile and delivery channel
- Treatment of the customer profiles and delivery channels

CONSEQUENCE

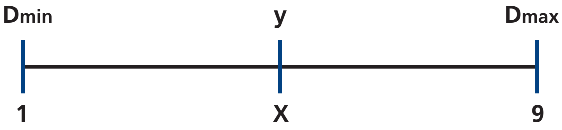
Consequence Factor Assessment

- Total suspicious financial transactions
- Total sales transactions

2. **Analysis,** Analysis is a core stage in the money laundering and terrorism financing risk assessment process. During this stage, due consideration is required concerning the nature, sources, likelihood and consequences of the risk factors that have been identified. Ultimately, the objective of this stage is to gain holistic understanding of each respective risk produced by the threat, vulnerability and consequence formula.

   Each determinant of key risk is transformed onto a scale of 1-9, where the data with the lowest value is automatically transformed to 1 on the scale and the data with the highest value is automatically transformed to 9. The remaining data is transformed to the 1-9 scale depending on the data value. The data is transformed using a simple mathematical formula as follows (Figure 1.3.2):

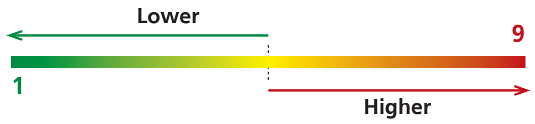
Figure 1.3.2.
Data Conversion Formula



$$X = \frac{8\,(y - D_{min})}{D_{max} - D_{min}}$$

For each key risk, the respective risk factors are totalled and averaged until the threats, vulnerabilities and consequences constitute scales from 1 to 9. In accordance with the risk assessment framework, the values obtained for the threats and vulnerabilities are subsequently totalled to produce the likelihood. Then, the likelihood value of each respective key risk is averaged and subsequently transformed to a 1-9 scale (Figure 1.3.3).

Figure 1.3.3.
Scale of Threats, Vulnerabilities, and Consequences



The likelihood value is multiplied by scale of consequences in order to produce a risk value. The scales for likelihood and consequence are both 1-9, therefore the smallest risk value is 1 (1x1) and the largest is 81 (9x9). The risk values are converted onto a 1-9 scale using the quadratic route of each risk value.

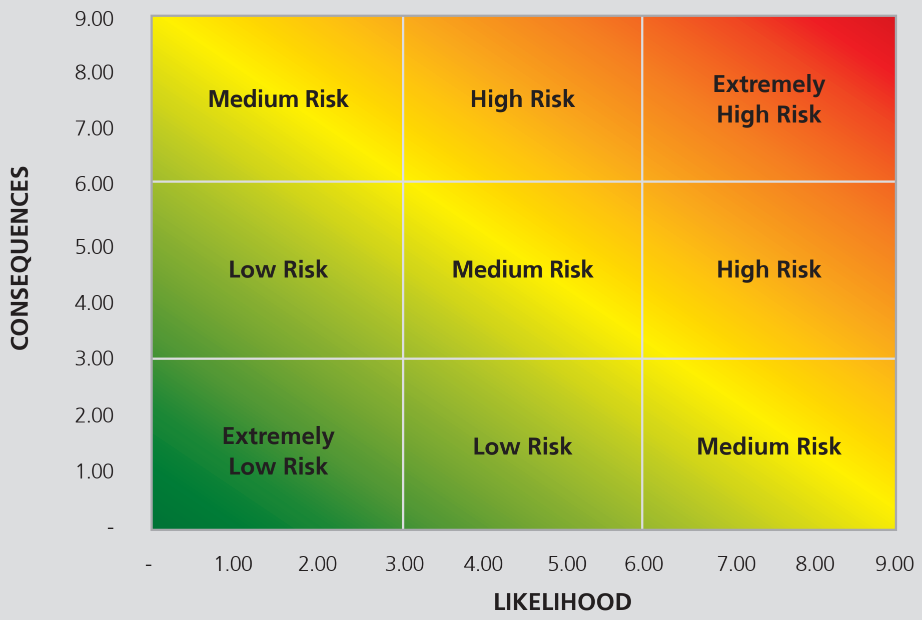
The risk assessment is divided into three levels, namely low, medium and high, with a 1-9 scale (Table 1.3.2).

Table 1.3.2.
Risk Level

Range of Risk Value	1 ≤ x < 3,67	3,67 ≤ x < 6,33	6,33 ≤ x ≤ 9
Risk Level	Low	Medium	High

3. **Evaluation** in the context of the money laundering and terrorism financing risk assessment process also encompasses the risk-taking analysed in the previous year to determine priority actions or build a prevention or risk avoidance strategy, as well as for risk mitigation or reduction and acceptance of low risk.

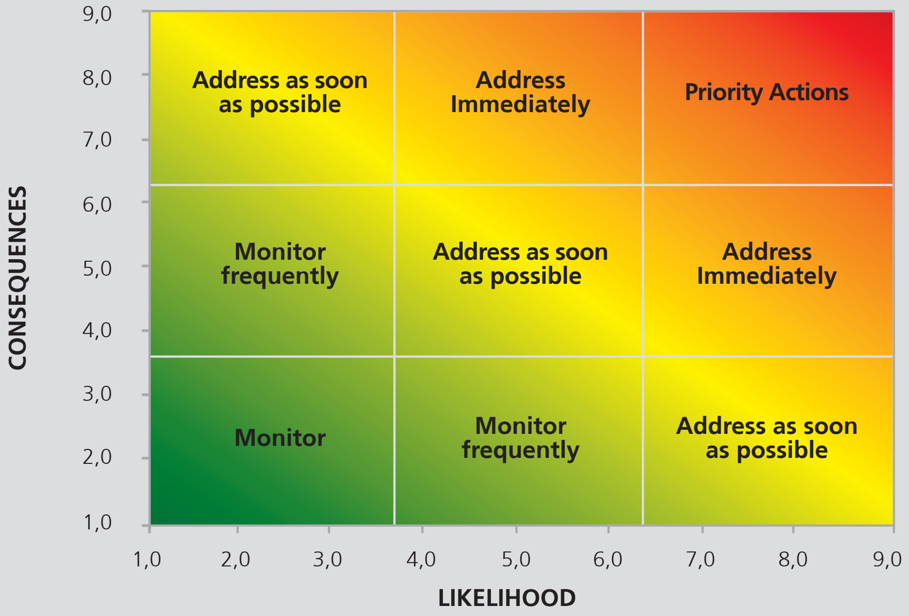
Figure 1.3.4.
Risk Matrix



To simplify the comparison between risk, likelihood and consequence of each respective key risk, the key risks are inputted into a risk graph, where the x-axis represents the likelihood and the y-axis represents the consequence (Figure 1.3.4).

The risk evaluation matrix as it pertains to assessing money laundering and terrorism financing risks is as follows (Figure 1.3.5):

Figure 1.3.5.
Risk Evaluation Matrix



B. Methodology Data

Quantitative and qualitative data for the period from 2015-2019 are used in this research of the ML and TF SRA, as the period after NRA implementation. The data was collected using questionnaires designed by INTRAC and distributed to industry players as the sample of this research.

C. Research Limitations

This review of the Sectoral Risk Assessment (SRA) of Money Laundering and Terrorism Financing was implemented after completion of the National Risk Assessment (NRA). The limitations of this research include:

1. The reporting parties used as respondents in this research were associated with a suspicious transaction frequency of more than 50%.
2. The Sectoral Risk Assessment was derived from the findings of the National Risk Assessment of ML and TF in 2015 and updated in 2019 (NRA 2015 Updated).

PART 2

Non-Bank
Money Changers

Executive Summary

In 2019, INTRAC together with other relevant government ministries/institutions updated the National Risk Assessment (NRA 2015 Updated). As a follow-up to mitigating money laundering and terrorism financing risk through Non-Bank Money Changers (KUPVA BB), a Sectoral Risk Assessment (SRA) of the industry was conducted. The objectives of the SRA are as follows:

1. To identify and analyse the threat of money laundering (ML) and terrorism financing (TF) in the Non-Bank Money Changers sector;
2. To identify than vulnerabilities and consequences of money laundering and terrorism financing through the Non-Bank Money Changers sector; and
3. To analyse the key risks of money laundering and terrorism financing.

The KUPVA BB Sectoral Risk Assessment (SRA) mapped three key risk areas, namely service user, location and product with the risk factors covering threats, vulnerabilities and consequences. The analysis method refers to the risk assessment published by the Financial Action Task Force (FATF). Based on the results of the assessment, the level of ML and TF risk in the Non-bank Money Changers sector was determined as follows:

1. **Jakarta** was identified as a **high-risk** region, followed by the **Riau Islands** and **Bali (medium risk)**. All other provinces in Indonesia were identified as low risk.
2. In terms of customer profile, **PEPs** and **Private Sector Employees** were considered **high risk,** followed by **entrepreneurs** and **housewives (medium risk)**. All other customer profiles were identified as low risk.
3. **USD** was considered a **high-risk** product (foreign banknote), followed by **SGD (medium risk)**. All other foreign banknotes were considered low risk.

In terms of ML and TF risk mitigation in the Non-Bank Money Changers sector, Bank Indonesia has issued regulations and guidelines as well as implemented on-site and off-site supervision. In conjunction with the National Police, Bank Indonesia has closed down unauthorised Non-Bank Money Changers throughout Indonesia. In addition, Bank Indonesia has also provided socialisation and education activities targeting Non-Bank Money Changers and the public in order to build awareness around ML and TF prevention and eradication.

1 LITERATURE REVIEW

A. Legal Basis

Bank Indonesia has been designated a Supervisory and Regulatory Body (LPP) for Non-Bank Money Changers in accordance with Act No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering. The provisions relating to Non-Bank Money Changers are contained within Bank Indonesia Regulation (PBI) No. 18/20/PBI/2016 concerning the Operating Activities of Non-Bank Money Changers (PBI KUPVA BB) and Bank Indonesia Circular No. 18/42/DKSP, dated 30th December 2016, regarding the Operating Activities of Non-Bank Money Changers (SEBI KUPVA BB). The provisions of the PBI KUPVA BB cover the following:

1. Scope of operating activities;
2. Submission requirements for underlying transactions;
3. Streamlining licensing procedures and requirements;
4. Governance and consumer protection; and
5. Buying and selling foreign banknotes by non-KUPVA BB.

B. Characteristics of Non-Bank Money Changers in Indonesia

1. Definition

KUPVA BB, or money changers, are non-bank business entities incorporated as limited companies that exchange foreign currencies[9]. The operating activities of money changes involve exchanging foreign banknotes (UKA)[10] as well as purchasing Travellers' Cheques. In addition, Non-Bank Money Changers also undertake other operating activities that are regulated by Bank Indonesia regulations[11], such as carrying foreign banknotes.

Any limited company wishing to operate as a money changer is first required to obtain a licence from Bank Indonesia. The operating licence issued by Bank Indonesia for a money changer is valid for five years and may be extended based on an application submitted by a money changer to Bank Indonesia. An authorised money changer is required to display the following:

a. An authorised money changer logo as issued by Bank Indonesia;
b. An operating licence certificate as issued by Bank Indonesia; and
c. "Authorised Money Changer" must be displayed prominently at the business location along with the name of the limited company.

Money changes are not permitted to:

a. Act as a selling agent for travellers' cheques;
b. Engage in margin, spot, forward and swap trading or other derivative transactions on behalf of a customer or the money changer itself;

[9] Article 1, paragraph 5 of Bank Indonesia Regulation (PBI) No.18/20/PBI/2016 concerning the Operating Activities of Non-Bank Money Changers (PBI KUPVA BB).

[10] According to Article 1, paragraph 1 of Bank Indonesia Regulation (PBI) No.18/20/PBI/2016 concerning the Operating Activities of Money Changers, UKA, or foreign banknotes, are official banknotes released by an issuing authority outside Indonesia and recognised as legal tender in the issuing country.

[11] Article 2, paragraph 2 of Bank Indonesia Regulation (PBI) No.18/20/PBI/2016 concerning the Operating Activities of Non-Bank Money Changers (PBI KUPVA BB).

c. Buy or sell foreign banknotes or purchase travellers' cheques from an unauthorised money changer;
d. Offer fund transfer activities; and
e. Engage in other operating activities beyond the operating activities of a money changer.

In addition, the directors, board of commissioners and/or shareholders of a money changer are prohibited from the following:

a. Owning an unauthorised money changer;
b. Cooperating with an unauthorised money changer; and
c. Conducting operating activities through an unauthorised money changer.

2. Products and Services

The recognised operating activities of KUPVA BB, or money changers, are as follows:

a. Exchanging foreign banknotes through a buy and sell mechanism;
b. Purchasing travellers' cheques.

The buying and selling mechanism for foreign banknotes is regulated as follows:

a. Foreign banknotes must be submitted physically in person;
b. Rupiah banknotes may be submitted physically in person or through an interbank or intrabank transfer;
c. An underlying transaction is required on foreign banknote purchases made by a Customer of a Money Changer exceeding a specific monthly threshold[12] per customer; and
d. The requirements referred to in letter c are not applicable if the foreign banknotes are purchased by an authorised money changer.

3. Regional Distribution

The number of authorised money changers in Indonesia is growing annually. According to the distribution data, most money changes are concentrated in the provinces of Jakarta, Riau Islands, Bali, East Java and West Java. The distribution of authorised money changes in Indonesia is summarised in the following table (Table 2.1.1).

Table 2.1.1.
Regional Distribution of Authorised Money Changers as of March 2019

Number	Region	Amount
1.	Jakarta Special Capital Region Province	401
2.	Riau Islands Province	163
3.	Bali Province	122
4.	East Java Province	118
5.	West Java Province	63
6.	North Sumatera Province	49
7.	Central Java Province	47
8.	Banten Province	44
9.	West Kalimantan Province	40
10.	Riau Province	18
11.	Yogyakarta Special Region Province	17
12.	West Nusa Tenggara Province	16
13.	Aceh Province	14
14.	West Sumatera Province	13
15.	Lampung Province	8
16.	South Sumatera Province	8
17.	East Nusa Tenggara Province	7
18.	Papua Province	7
19.	South Sulawesi Province	5
20.	North Sulawesi Province	3
21.	Jambi Province	2
22.	North Kalimantan Province	2
23.	Bengkulu Province	1
24.	South Kalimantan Province	1
25.	East Kalimantan Province	1
26.	Maluku Province	1
27.	North Maluku Province	1
	Total	**1171**

Source: Bank Indonesia

[12] The threshold for foreign banknote purchases by the Customer of a Money Changer refers to prevailing Bank Indonesia regulations concerning foreign currency transactions against the rupiah between banks with domestic parties as well as foreign parties. Currently, the threshold is USD25,000 or equivalent in accordance with Bank Indonesia Regulation (PBI) No. 18/19/PBI/2016.

2 KEY RISKS IN THE NON-BANK MONEY CHANGERS SECTOR

A. ML Risk Landscape in the Non-Bank Money Changers Sector

The modus operandi of money laundering in Indonesia has become increasingly complex and diverse over time. Financial institutions as well as non-financial institutions may be exploited for money laundering purposes. Based on the results of a National Risk Assessment (NRA) of ML, the predicate offence of most money laundering cases in Indonesia is dominated by narcotics, corruption, banking crime, tax fraud, deforestation/illegal logging and the capital market. Money laundering is used to conceal the origins of illegally obtained money.

Based on a literature review, the dominant predicate offences of most money laundering activity through Non-Bank Money Changers are corruption and narcotics. Most offenders are entrepreneurs and private sector employees, with the majority located in Jakarta. According to INTRAC data, the modi operandi of money laundering activity through money changers are as follows:

1. Purchase of foreign banknotes not by the beneficial owner.
2. Transactions processed not matching user profile.
3. Large cash purchases of foreign banknotes.
4. Exchange of significant foreign banknotes of different currencies in one transaction.
5. Exchange of significant foreign banknotes by a Politically Exposed Person (PEP).
6. Significant transactions without a clear underlying transaction.
7. Use of individual/private accounts for Non-Bank Money Changers operating activities to collect proceeds of crime.
8. Use of unauthorised money changers.
9. Use of fraudulent identification when exchanging foreign currency.
10. Exchange of large-denomination foreign banknotes, such as SGD10,000.
11. Low-value, high-frequency transactions (structuring).

B. TF Risk Landscape in the Non-Bank Money Changers Sector

Terrorism financing through the Non-Bank Money Changers sector aims to exchange foreign banknotes into rupiah and vice versa in order to facilitate terrorism financing. Based on a literature review, incidents of terrorism financing through money changers primarily occurred in Jakarta, dominated by entrepreneurs.

According to INTRAC data, the modi operandi of terrorism financing activity through money changers are as follows:

1. Purchase of foreign banknotes not by the beneficial owner.
2. Transactions processed not matching user profile.
3. Low-value, high-frequency transactions (structuring).

C. ML and TF Risk Assessment in the Non-Bank Money Changers Sector

1. Risk by Region

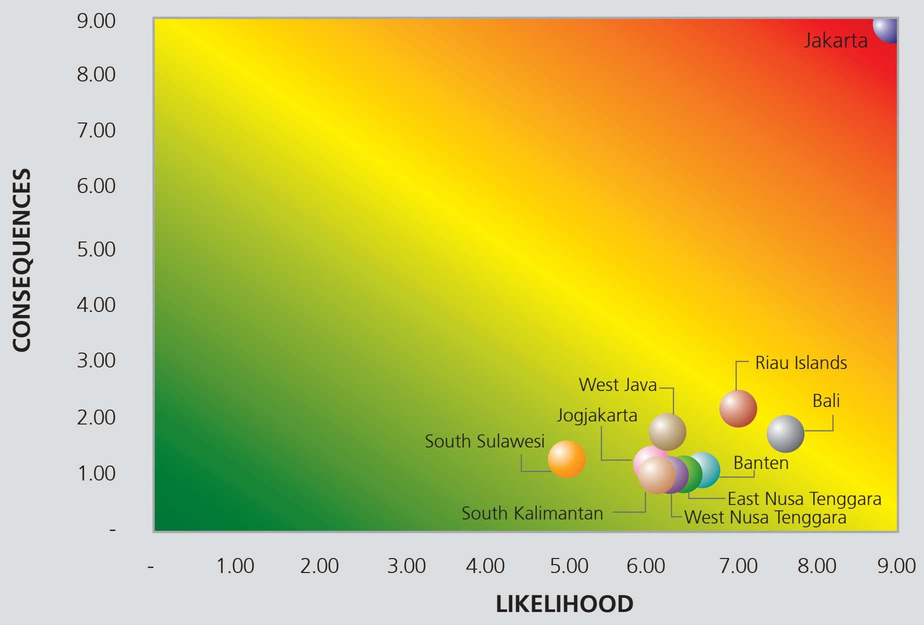
A regional assessment of ML and TF risks in the Non-Bank Money Changers sector was conducted to explore which regions (provinces) were most at risk to cases of ML and TF. Risk was assessed as a function of threat, vulnerability and consequence in each respective province, with the three aspects measured based on predetermined risk factors.

The level of risk by region was calculated as a function of multiplying the likelihood by the consequences in each respective province, where the likelihood is the sum of the threat and vulnerability. The following heat map illustrates ML and TF risks in the Non-Bank Money Changers sector by region expressed as a function of threat, vulnerability and consequence (Figure 2.1.1):

Jakarta's position on the x-axis of the heat map revealed a higher likelihood than the other regions. Furthermore, the position on the y-axis showed that the consequences of ML and TF activity in the Non-Bank Money Changers sector in Jakarta was also highest compared with other regions.

The provinces of Bali and Riau Islands were considered medium risk to ML and TF incidences in the Non-Bank Money Changers sector. In terms of threat and vulnerability, Bali received a medium score due to the high number of money changers located in the region. Notwithstanding, the consequences in Bali were assessed to be low in line with the low transaction value compared with conditions in Jakarta as a region identified with a high consequence level. Similar to Bali, the Riau Islands were considered to have medium levels of threat and vulnerability, together with a low consequence level.

Figure 2.1.1.
Risk by Region



According to the heat map of risk presented above, Jakarta was considered high risk in terms of ML and TF incidences in the Non-Bank Money Changers sector. On the other hand, the medium-risk regions were the Riau Islands and Bali, while all other provinces were deemed low risk.

The values for threat and consequence were highest in Jakarta, coupled with a medium level of vulnerability.

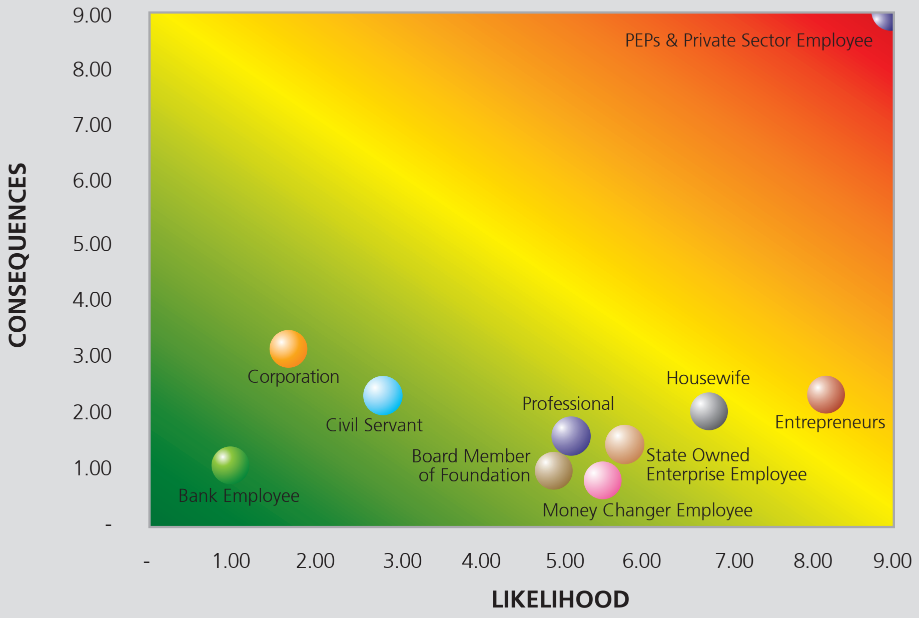
2. **ML and TF Risk by Customer Profile**

   ML and TF risk were also assessed based on customer profile in order to investigate which profiles (professions) were most at risk to ML and TF in the Non-Bank Money Changers sector. The types of customer profile assessed were those identified in the NRA as high and medium risk of perpetrating ML and TF. The risk assessment based on customer profile in the Non-Bank Money Changers sector faced the following limitations:

   a. The requirement for Non-Bank Money Changers to administrate information concerning services users in accordance with Article 51, paragraph (1) of Bank Indonesia Regulation (PBI) No. 19/10/PBI/2017 regarding Anti-Money Laundering and Countering Terrorism Financing (AML/CFT) for Payment System Service Providers and Non-Bank Money Changers.
   b. The dominance of walk-in customers in the Non-Bank Money Changers sector.
   c. The questionnaire did not explicitly measure Politically Exposed Persons (PEP) because PEPs are directly categorised as high-risk customers.

The level of risk based on customer profile was calculated as a function of multiplying the likelihood by the consequences for each respective profile, where the likelihood is the sum of the threat and vulnerability. The following heat map illustrates ML and TF risks in the Non-Bank Money Changers sector by customer profile expressed as a function of threat, vulnerability and consequence (Figure 2.1.2):

Figure 2.1.2.
Risk by Customer Profile



According to the heat map of risk presented above, the customer profile considered high risk in terms of ML and TF activity in the Non-Bank Money Changers sector was Private Sector Employees, while the medium-risk customer profiles were Entrepreneurs and Housewives and all other customer profiles were deemed low risk.

Private Sector Employees received the highest threat, consequence and vulnerability scores. The position of Private Sector Employees on the x-axis of the heat map demonstrated a higher likelihood than the other profiles. Meanwhile, the position of Private Sector Employees on the y-axis of the heat map shows that the consequence of ML and TF activity in the Non-Bank Money Changers sector by Private Sector Employees was highest compared with other customer profiles.

In accordance with Article 34 of Bank Indonesia Regulation (PBI) No. 19/10/PBI/2017 concerning Anti-Money Laundering and Countering Terrorism Financing (AML/CFT) for Payment System Service Providers and Non-Bank Money Changers, and in reference to FATF Guidance on Politically Exposed Persons that states PEPs are particularly vulnerable to money laundering, prospective service users, service users and beneficial owners that are categorised as PEPs were also considered high-risk customer profiles.

Entrepreneurs and Housewives were considered medium risk in terms of ML and TF in the Non-Bank Money Changers sector. Regarding the threat and consequences, Entrepreneurs received medium scores, yet a high value for vulnerability. Meanwhile, Housewives in the Non-Bank Money Changers sector were high risk in terms of vulnerability, yet low risk in terms of threat and consequences.

3. ML and TF Risk by Product

ML and TF risk were assessed on a product-by-product basis in order to explore which products were most at risk to ML and TF cases in the Non-Bank Money Changers sector. The only product of the Non-Bank Money Changers sector is foreign banknotes, therefore, risk was assessed based on the 10 major foreign banknotes traded in the KUPVA BB sector.

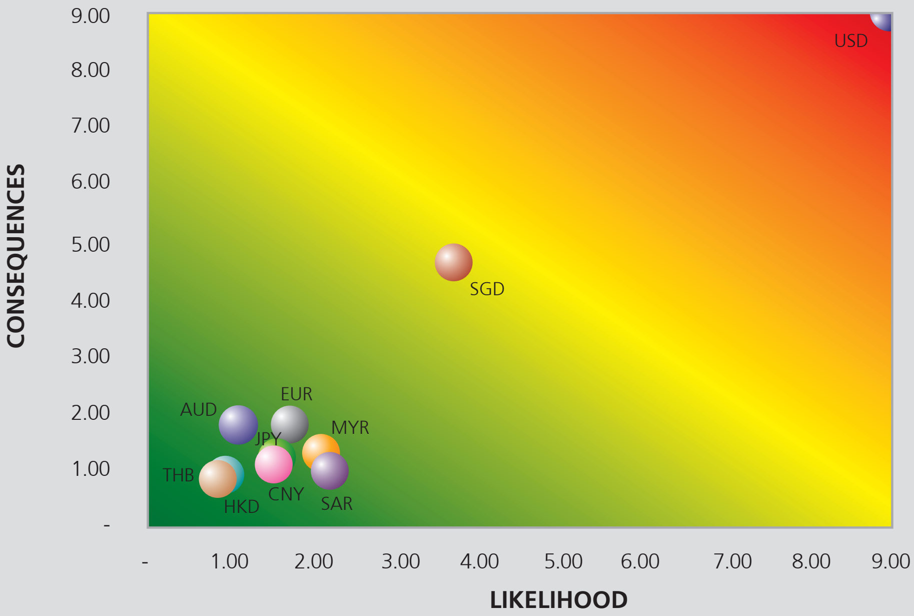
The level of risk based on product (foreign banknote) was calculated as a function of multiplying the likelihood by the consequences for each respective currency, where the likelihood is the sum of the threat and vulnerability. The following heat map illustrates ML and TF risks in the Non-Bank Money Changers sector by product expressed as a function of threat, vulnerability and consequence (Figure 2.1.3):

According to the heat map of risk presented below, the product considered high risk in terms of ML and TF cases in the Non-Bank Money Changers sector was USD, while the SGD was considered a medium-risk product and all other products (foreign banknotes) were deemed low risk.

US dollars had the highest threat and consequence values compared with other banknote currencies. The position of USD on the x-axis of the heat map demonstrated a higher likelihood than the other currencies. Meanwhile, the position on the y-axis of the heat map showed that the consequences of ML and TF cases in the Non-Bank Money Changers sector using US dollar banknotes was highest compared with the other currencies.

Singapore dollars (SGD) were considered medium risk of ML and TF in the Non-Bank Money Changers sector due to the medium consequence score because Singaporean dollars are the second most popular currency exchanged by money changers after US dollars.

Figure 2.1.3.
Risk by Product (Foreign Banknote)



3 RISK MITIGATION

A. Risk Mitigation: Institutional Aspects

1. Non-Bank Money Changers operating in Indonesia are required to hold a licence from Bank Indonesia.
2. Non-Bank Money Changers in Indonesia are prohibited from other business activities, including fund transfers.
3. Non-Bank Money Changers, the management and shareholders are prohibited from business relations or transacting with unauthorised money changers.
4. The management and shareholders of Non-Bank Money Changers are required to meet certain requirements as stipulated by Bank Indonesia as follows:
   a. not registered on the National Blacklist (DHN)[13];
   b. not constrained by non-performing loans based on the debtor information system;
   c. fulfilling tax obligations based on a fiscal statement issued by the tax authority for the previous 1 year;
   d. not convicted of certain crimes within the past two years;
   e. not a shareholder, director or board member of a Limited Company that has been the subject of administrative sanctions in the form of business licence revocation by Bank Indonesia in the two years prior to submitting the application;
   f. never been declared bankrupt;
   g. not a shareholder, director or board member found liable of causing bankruptcy in the two years prior to submitting the application;
5. Shareholders of Non-Bank Money Changers must be Indonesian citizens and/or business entities where the shares are held in entirety by Indonesian citizens.
6. Paid-up capital for Non-Bank Money Changers must not originate from and/or be used for money laundering purposes.
7. A Non-Bank Money Changers operating license is valid for 5 years and may be extended based on an application submitted to Bank Indonesia.
8. Non-Bank Money Changers are required to maintain a bank account in the name of the Non-Bank Money Changers.

B. Risk Mitigation: Product Features

1. The operating activities of Non-Bank Money Changers are restricted to:
   a. exchanging foreign banknotes; and
   b. purchasing travellers' cheques.
2. Foreign banknotes must be submitted physically in person.
3. If rupiah currency is submitted via interbank or intrabank transfer, the currency must originate or be transferred to the Non-Bank Money Changers's bank account.
4. Customers purchasing foreign banknotes exceeding USD25,000 or equivalent in one month are required to submit an underlying transaction.
5. Non-Bank Money Changers are prohibited from recirculating SGD10,000 banknotes.

[13] In accordance with Bank Indonesia Regulation (PBI) No. 18/43/PBI/2016 as an amendment to Bank Indonesia Regulation (PBI) No. 8/29/PBI/2006 concerning the National Blacklist, the National Blacklist contains information regarding all parties withdrawing bad cheques.

C. Risk Mitigation: Operational Aspects

1. The Directors and Board of Commissioners are required to supervise AML/CFT program implementation.
2. Non-Bank Money Changers are required to implement identification and verification; manage the data, information and documents; as well as report to the authorities.
3. Non-Bank Money Changers are required to implement more rigorous identification procedures for high-risk Prospective Service Users, Service Users and Beneficial Owners.
4. Non-Bank Money Changers are required to identify and report suspicious financial transactions to INTRAC.
5. Non-Bank Money Changers are required to identify, assess, control and mitigate the risks.
6. Non-Bank Money Changers are required to implement employee screening, monitor employee profiles and provide capacity building to employees.
7. Non-Bank Money Changers are required to apply internal controls, for example a periodic independent audit, to test AML/CFT compliance and implementation.
8. Non-Bank Money Changers are require to administrate, update and check the List of Suspected Terrorist Organisations and Individuals (DTTOT) and the list of financing of proliferation of weapons of mass destruction against customer information.

D. Risk Mitigation: Oversight

1. Bank Indonesia implements on-site and off-site risk-based supervision of AML/CFT implementation by Non-Bank Money Changers.
2. Bank Indonesia implements thematic supervision of Non-Bank Money Changers.
3. Bank Indonesia may appoint a third party to inspect a Non-Bank Money Changers on behalf of Bank Indonesia.
4. For oversight by Bank Indonesia, Non-Bank Money Changers are required to identify, administrate and update data on beneficial owners, while ensuring the availability of such data to Bank Indonesia for supervision purposes.

4 CONCLUSION

Based on the analysis of statistical data and professional judgement to measure sectoral risk in the Non-Bank Money Changers sector based on location, customer profile and product, the following conclusions were drawn (Table 2.1.2):

1. **Jakarta** was considered a **high-risk** region for ML and TF activity in the KUPVA BB sector, followed by the **Riau Islands** and **Bali** as medium-risk provinces. All other provinces were considered low risk.
2. In terms of customer profile, **PEPs** and **Private Sector Employees** were considered high risk for ML and TF activity in the KUPVA BB sector, followed by **entrepreneurs** and **housewives** (**medium** risk). All other customer profiles were considered low risk.
3. USD was considered a **high**-risk product (foreign banknote) for ML and TF activity in the KUPVA BB sector, followed by **SGD** (**medium** risk). All other foreign banknotes were considered low risk.

Table 2.1.2.
SRA Results for Non-Bank Money Changers

SRA Non-Bank Money Changers			
Risk	**Location**	**Customer**	**Product**
High	Jakarta	PEP and Private Sector Employees	USD
Medium	Riau Islands & Bali	Entrepreneurs & Housewifes	SGD
Low	Others	Others	Others

Non-Bank
Money Transfer Services Providers

Executive Summary

In 2019, the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC) in conjunction with relevant government ministries/institutions updated the National Risk Assessment (NRA 2015 Updated). As a follow-up risk-mitigation action against money laundering and terrorism financing at Non-Bank Money Transfer Services Providers (MVTS), a sectoral risk assessment was conducted. The Sectoral Risk Assessment (SRA) was compiled with the following objectives:

1. To identify and analyse the threat of money laundering (ML) and terrorism financing (TF) in the MVTS sector;
2. To identify than vulnerabilities and consequences of money laundering and terrorism financing through the MVTS sector; and
3. To analyse the key risks of money laundering and terrorism financing.

The Non-Bank MVTS Sectoral Risk Assessment (SRA) mapped three key risk areas, namely service user, location and product with the risk factors covering threats, vulnerabilities and consequences. The analysis method refers to the risk assessment published by the Financial Action Task Force (FATF). Based on the results of the assessment, the level of ML and TF risk in the Non-Bank MVTS sector was determined as follows:

1. **Jakarta** and **East Java** were considered high-risk regions, followed by **Central Java** (**medium** risk). All other provinces in Indonesia were identified as low risk.
2. In terms of customer profile, **PEPs** and **Private Sector Employees** were considered **high** risk, followed by **entrepreneurs, housewives** and **Board Member of Foundation** (**medium** risk). All other customer profiles were identified as low risk.
3. **Incoming** was the MVTS product identified as **high** risk, followed by **outgoing** and **domestic** that were identified as low risk.

In terms of ML and TF risk mitigation in the Non-Bank MVTS sector, Bank Indonesia has issued regulations and guidelines as well as implemented on-site and off-site supervision. In conjunction with the National Police, Bank Indonesia has closed down unauthorised MVTS operating throughout Indonesia. In addition, Bank Indonesia has also provided socialisation and education activities targeting MVTS and the public in order to build awareness around ML and TF prevention and eradication.

1 | LITERATURE REVIEW

A. Legal Basis

Bank Indonesia has been designated a Supervisory and Regulatory Body (LPP) for Non-Bank Money Transfer Services Providers in accordance with Act No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering. Fund transfer activity is regulated pursuant to the Fund Transfer Act (No. 3) of 2011. Pursuing its mandate in accordance with the Fund Transfer Act, Bank Indonesia issued Bank Indonesia Regulation (PBI) No. 14/23/PBI/2012 concerning Fund Transfers and Bank Indonesia Circular Letter (SEBI) No. 15/23/DASP regarding Fund Transfers. The provisions of the Bank Indonesia regulations are as follows:

1. Licensing of Non-Bank Money Transfer Services Providers;
2. Transferring funds;
3. Transferring funds for receipt in cash;
4. Services, interest or compensation;
5. Fund transfer fees;
6. Monitoring; and
7. Sanctions.

B. Characteristics of Non-Bank MVTS in Indonesia

1. Definition

Article 1, paragraph (2) of the Fund Transfer Act (No. 3) of 2011 states that Money Transfer Services Providers are banks and non-bank business entities engaged in fund transfer activities. Banks are not required to hold a licence to transfer funds because such activities are already part of the operating activities of a bank and, thus, regulated by prevailing laws.

Nevertheless, Non-Bank Money Transfer Services Providers are required to obtain a licence from Bank Indonesia through a written application submitted to Bank Indonesia. Non-Bank Money Transfer Services Providers are also required to meet the following requirements as contained in Bank Indonesia regulations: (i) system security; (ii) capital; (iii) management integrity; (iv) risk management; and (v) infrastructure availability.

A fund transfer is initiated when a transfer instruction has been issued to the originator and forwarded to a financial institution and the recipient. In accordance with the Fund Transfer Act, Bank Indonesia implements on-site and off-site supervision. On-site supervision is implemented periodically and/or as required, whereas off-site supervision is achieved through monitoring the reports submitted by money transfer services providers.

2. Products and Services

The products and services offered by Non-Bank Money Transfer Services Providers include:

a. Outgoing transfers (Indonesia to international);
b. Incoming transfers (International to Indonesia); and
c. Domestic transfers (within Indonesia).

3. Regional Distributions

Most MVTS are concentrated in Jakarta, Riau Islands, West Java, North Sumatra and East Java as follows (Table 2.2.1):

Table 2.2.1.
Regional Distribution of MVTS as of March 2019

Number	Region	Amount
1.	Jakarta Special Capital Region Province	69
2.	Riau Islands Province	34
3.	West Java Province	12
4.	East Java Province	8
5.	North Sumatera Province	8
6.	West Kalimantan Province	5
7.	Central Java Province	3
8.	West Nusa Tenggara Province	2
9.	Bali Province	1
10.	West Sumatera Province	1
	Total	**143**

Source: Bank Indonesia

2 KEY RISKS IN THE NON-BANK MVTS SECTOR

A. ML Risk Landscape in the Non-Bank MVTS Sector

The modus operandi of money laundering in Indonesia has become increasingly complex and diverse over time. Financial institutions as well as non-financial institutions may be exploited for money laundering purposes. Based on the results of a National Risk Assessment (NRA) of ML, the predicate offences of most money laundering cases in Indonesia are dominated by narcotics, corruption, banking crime, tax fraud, deforestation/illegal logging and the capital market. Money laundering is used to conceal the origins of illegally obtained money.

ML activity exploits the Non-Bank MVTS sector in order to conceal the origins of illegally obtained money. ML perpetrators send and/or receive funds through Non-Bank MVTS to exploit industry weaknesses through specific modi operandi. Over time, the modus operandi of money-laundering in Indonesia has involved diverse cross-border transactions, through the Non-Bank MVTS sector in particular.

Based on information from INTRAC, the various modi operandi for ML activity through the Non-Bank MVTS sector are as follows:

1. A licensed Non-Bank MVTS cooperating with an unauthorised Non-Bank MVTS to send or receive funds;
2. Low-value, high-frequency transactions (structuring);
3. Outgoing transactions through several Non-Bank MVTS to the same recipient;
4. Non-Bank MVTS transactions that are not consistent with operating activities. For instance, a Non-Bank MVTS established to provide remittance transfer services for Indonesian migrant workers placed in Hong Kong, yet no significant incoming foreign currency transfers are recorded, with incoming transactions dominated by domestic transfers.

Referring to the literature review, Non-Bank MVTS were exploited in ML cases with the predicate offence dominated by tax fraud. Furthermore, most perpetrators of ML crime in the Non-Bank MVTS sector were entrepreneurs and located in Jakarta.

B. TF Risk Landscape in the Non-Bank MVTS Sector

TF perpetrators use the Non-Bank MVTS sector to send and/or receive funds for terrorism financing. Funds are sent and/or received domestically and internationally. ML offenders exploit industry weaknesses through specific modi operandi to finance terrorism. Based on the NRA of TF, Non-Bank MVTS are at risk when moving funds internationally to finance terrorism.

The modus operandi of terrorism financing Indonesia has evolved over time and involves cross-border transactions. Based on information from INTRAC, the following modi operandi have been identified in the Non-Bank MVTS sector:

1. A licensed Non-Bank MVTS cooperating with an unauthorised Non-Bank MVTS to send or receive funds;

2. Low-value, high-frequency transactions (structuring);
3. Higher frequency incoming transfers from several high-risk countries;
4. Outgoing transfers through several Non-Bank MVTS to the same recipient; and
5. Cuckoo smurfing, which involves the concealment of the origins of illegally obtained money through an unsuspecting third-party account.

Referring to the literature review, most TF cases involved Non-Bank MVTS located in Jakarta. Furthermore, most TF crime in the Non-Bank MVTS sector was committed by entrepreneurs.

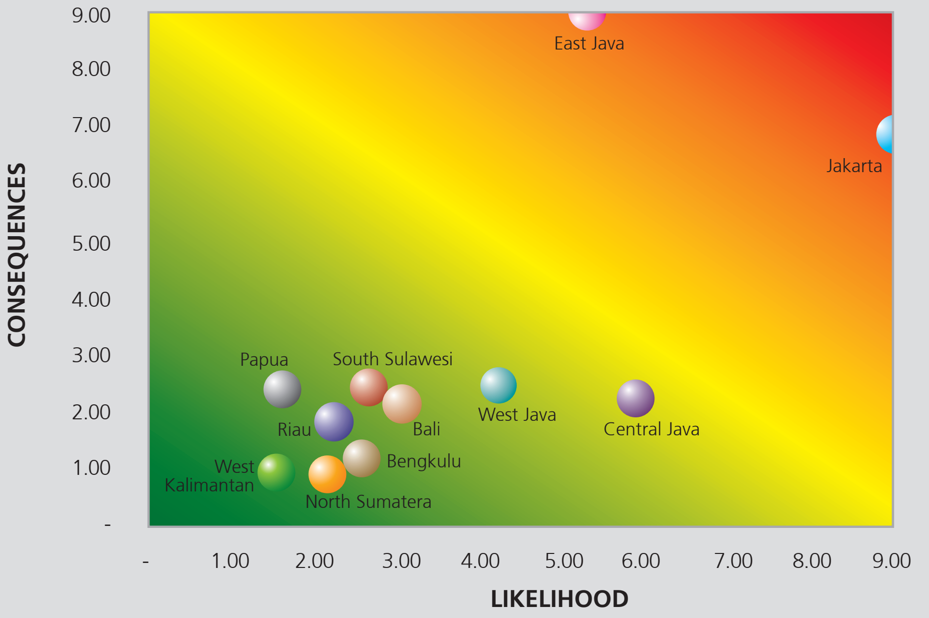
C. ML and TF Risk Assessment in the Non-Bank MVTS Sector

1. ML and TF Risk by Region

A regional assessment of ML and TF risks in the Non-Bank MVTS sector was conducted to explore which regions (provinces) were most at risk to cases of ML and TF. The objects of the regional risk assessment were identified as medium and high-risk provinces of ML and TF incidences in Indonesia based on the NRA. Risk was assessed as a function of threat, vulnerability, and consequence in each respective province, with the three aspects measured based on predetermined risk factors.

The level of risk by region was calculated as a function of multiplying the likelihood by the consequences in each respective province, where the likelihood is the sum of the threat and vulnerability. The following heat map illustrates ML and TF risks in the Non-Bank MVTS sector by region expressed as a function of threat, vulnerability and consequence (Figure 2.2.1):

Figure 2.2.1.
Risk by Region



According to the heat map of risk presented above, **Jakarta** and **East Java** were considered **high risk** in terms of ML and TF activity in the MVTS sector. On the other hand, **Central Java** was identified as a **medium-risk** region, while the 25 other provinces were deemed low risk.

The values for threat and consequence were highest in Jakarta and East Java, together with a medium level of vulnerability. The positions of Jakarta and East Java on the x-axis of the heat map revealed a higher likelihood than other regions. Furthermore, the respective positions on the y-axis showed that the consequence of ML and TF in the Non-Bank MVTS sector were also highest in Jakarta and East Java compared with the other provinces.

The province of Central Java was identified as medium risk to ML and TF incidences in the Non-Bank MVTS sector. In terms of threat and vulnerability, Central Java was medium risk due to the high number of Non-Bank MVTS service points located in the region. Notwithstanding, the consequences in Central Java were assessed to be low in line with the low transaction value compared with conditions in Jakarta and East Java as regions assessed to have a high consequence level.

2. **ML and TF Risk by Customer Profile**

   ML and TF risk were also assessed based on customer profile in order to investigate which profiles (professions) were most at risk to ML and TF in the Non-Bank MVTS sector. The types of customer profile assessed were those identified in the NRA as high and medium risk of committing ML and TF. The risk assessment based on customer profile in the Non-Bank MVTS sector faced the following limitations:

   a. The requirement for MVTS to administrate information concerning services users in accordance with Article 51, paragraph (1) of Bank Indonesia Regulation (PBI) No. 19/10/PBI/2017 regarding Anti-Money Laundering and Countering Terrorism Financing (AML/CFT) for Payment System Service Providers and KUPVA BB.
   b. The dominance of walk-in customers in the Non-Bank MVTS sector.
   c. The questionnaire did not explicitly measure Politically Exposed Persons (PEP) because PEPs are directly categorised as high-risk customers.

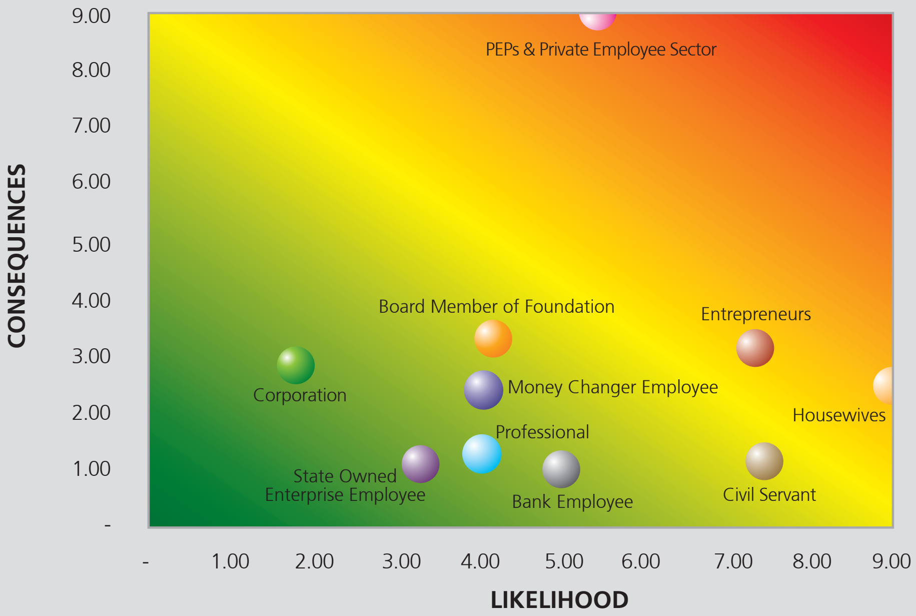
The level of risk based on customer profile was calculated as a function of multiplying the likelihood by the consequences for each respective profile, where the likelihood is the sum of the threat and vulnerability. The following heat map illustrates ML and TF risks in the Non-Bank MVTS sector by customer profile expressed as a function of threat, vulnerability and consequence (Figure 2.2.2):

According to the heat map of risk presented below, the customer profile considered **high risk** in terms of ML and TF in the Non-Bank MVTS sector was **Private Sector Employees,** while the **medium-risk** customer profiles were **Entrepreneurs, Housewives** and **Board Member of Foundation** and all other customer profiles were deemed low risk.

Private Sector Employees had the highest threat, consequence and vulnerability scores compared with other customer profiles that received medium scores. The position of Private Sector Employees on the x-axis of the heat map demonstrated a higher likelihood than the other profiles. Notwithstanding, the position of Private Sector Employees on the y-axis of the heat map showed that the consequence of ML and TF in the Non-Bank MVTS sector by Private Sector Employees was medium compared with other customer profiles.

In accordance with Article 34 of Bank Indonesia Regulation (PBI) No. 19/10/PBI/2017 concerning Anti-Money Laundering and Countering Terrorism Financing (AML/CFT) for Payment System Service Providers and KUPVA BB, and in reference to FATF Guidance on Politically Exposed Persons that states

Figure 2.2.2.
Risk by Customer Profile



PEPs are particularly vulnerable to money laundering, prospective service users, service users and beneficial owners that are categorised as PEPs were also considered high-risk customer profiles.

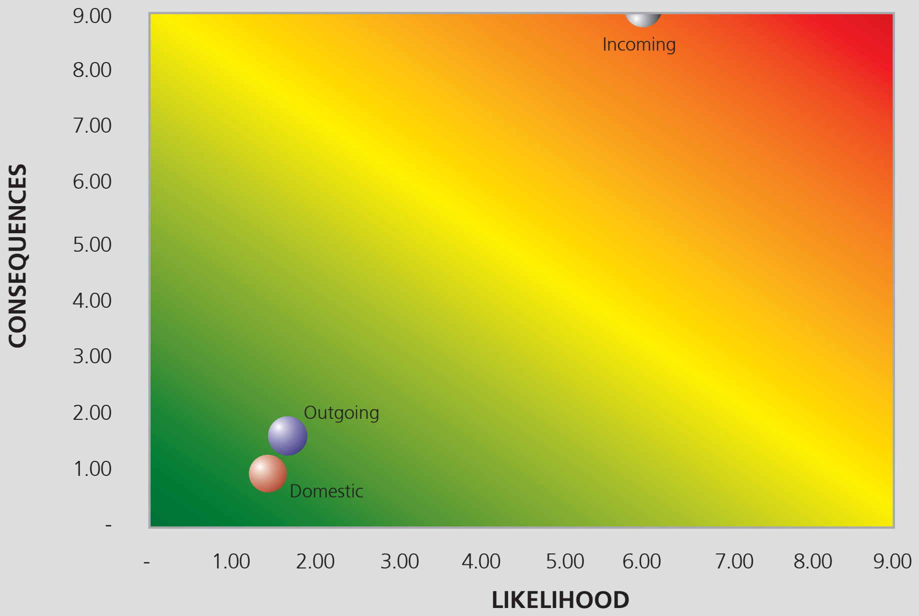
Entrepreneurs, Housewives and Board Member of Foundation were considered medium risk in terms of ML and TF activity in the Non-Bank MVTS sector. Regarding the threat and consequences, Entrepreneurs received medium scores because the total and value of suspicious financial transactions made by entrepreneurs reported to INTRAC by Non-Bank MVTS as well as total customers and the transaction value pertaining to the entrepreneur customer profile in the Non-Bank MVTS sector were the second highest after Private Sector Employees. Meanwhile, Housewives in the Non-Bank MVTS sector were high risk in terms of vulnerability, yet received medium scores in terms of threat and consequences.

3. ML and TF Risk by Product

ML and TF risk were assessed on a product-by-product basis in order to explore which products were most at risk to ML and TF cases in the Non-Bank MVTS sector. Non-Bank MVTS products include receiving international transfers to Indonesia (incoming), sending international transfers from Indonesia (outgoing) as well as sending and receiving transfers within the territory of the Republic of Indonesia (domestic). Consequently, risk was assessed based on those three products.

The level of risk based on product was calculated as a function of multiplying the likelihood by the consequences for each respective product, where the likelihood is the sum of the threat and vulnerability. The following heat map illustrates ML and TF risks in the Non-Bank MVTS sector by product expressed as a function of threat, vulnerability and consequence (Figure 2.2.3):

Figure 2.2.3.
Risk by Product



According to the heat map of risk presented above, the product considered **high risk** in terms of ML and TF activity in the Non-Bank MVTS sector was **incoming transfers,** while **outgoing** and **domestic transfers** were considered **low-risk** products.

Incoming transfers had the highest threat and consequence values compared to other Non-Bank MVTS products. The position of incoming transfers on the x-axis of the heat map demonstrated a higher likelihood than the other products. Meanwhile, the position on the y-axis of the heat map showed that the consequences of ML and TF in the Non-Bank MVTS sector through incoming transfers were highest compared with the other products.

3 RISK MITIGATION

A. Risk Mitigation: Institutional Aspect

1. Non-Bank MVTS operating in Indonesia are required to obtain a licence from Bank Indonesia.
2. Non-Bank MVTS must be legally incorporated in Indonesia.
3. Licence applications must be complemented with the following documents and/or requirements: documents relating to institutional and financial conditions, as well as documents pertaining to operational preparedness.
4. The management and owners of Non-Bank MVTS are required to meet certain requirements as stipulated by Bank Indonesia as follows:
    a. never been declared bankrupt or a director or board member found liable of causing bankruptcy in the five years prior to submitting the application;
    b. never been convicted for banking or financial crimes or money laundering;
    c. not listed on the credit blacklist at time of application; and
    d. not registered on the National Blacklist.
5. Non-Bank MVTS are prohibited from transacting with unauthorised Non-Bank MVTS.

B. Risk Mitigation: Product Features

Bank Indonesia is authorised to stipulate the maximum value of international funds transfers processed through the Non-Bank MVTS sector.

C. Risk Mitigation: Operational Aspect

1. The Directors and Board of Commissioners are required to supervise AML/CFT program implementation.
2. Non-Bank MVTS are required to implement identification and verification; manage the data, information and documents; as well as report to the authorities.
3. Non-Bank MVTS are required to implement more rigorous identification procedures for high-risk Prospective Service Users, Service Users and Beneficial Owners.
4. Non-Bank MVTS are required to identify and report suspicious financial transactions to INTRAC.
5. Non-Bank MVTS are required to identify, assess, control and mitigate the risks.
6. Non-Bank MVTS are required to implement employee screening, monitor employee profiles and provide capacity building to employees.
7. MVTS are required to apply internal controls, for example a periodic independent audit, to test AML/CFT compliance and implementation.
8. MVTS are require to administrate, update and check the List of Suspected Terrorist Organisations and Individuals (DTTOT) and the list of financing of proliferation of weapons of mass destruction against customer information.

D. Risk Mitigation: Oversight

1. Bank Indonesia implements on-site and off-site risk-based supervision of AML/CFT implementation by Non-Bank MVTS.
2. Bank Indonesia implements thematic supervision of Non-Bank MVTS.
3. Bank Indonesia may appoint a third party to inspect a Non-Bank MVTS on behalf of Bank Indonesia.
4. For oversight by Bank Indonesia, Non-Bank MVTS are required to identify, administrate and update the data on beneficial owners, while ensuring the availability of such data to Bank Indonesia for supervision purposes.

4 CONCLUSION

Based on the analysis of statistical data and professional judgement to measure sectoral risk at Non-Bank MVTS based on location, customer profile and product, the following conclusions were drawn (Table 2.2.2):

1. **Jakarta** and **East Java** were considered **high-risk** regions in terms of ML and TF activity in the Non-Bank MVTS sector, followed by **Central Java** (**medium risk**). All other provinces in Indonesia were identified as **low risk**.
2. Regarding customer profile, **PEPs** and **Private Sector Employees** were considered **high risk** in terms of ML and TF activity in the Non-Bank MVTS sector, followed by **entrepreneurs, housewives** and **Board Member of Foundation** (**medium risk**). All other customer profiles were identified as low risk.
3. **Incoming** transfers were the Non-Bank MVTS product identified as **high** risk in terms of ML and TF activity in the Non-Bank MVTS sector, followed by **outgoing** and **domestic** transfers that were identified as **low** risk.

Table 2.2.2.
SRA Results for Non-Bank MVTS

SRA Non-Bank MVTS

Risk	Location	Customer	Product
High	Jakarta & East Java	PEPs & Private Sector Employees	Incoming Transfer
Medium	Central Java	Entrepreneurs, Housewives, Board Member of Foundation	-
Low	Others	Others	Outgoing and Domestic Transfer

Non-Bank
E-Money and E-Wallet Issuers

Executive Summary

In 2019, the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC) in conjunction with relevant government ministries/institutions updated the National Risk Assessment (NRA 2015 Updated). As a follow-up risk-mitigation action against money laundering and terrorism financing at Non-Bank e-Money and e-Wallet Issuers (Non-Bank EM and EW), a sectoral risk assessment was conducted. The Sectoral Risk Assessment (SRA) was compiled with the following objectives:

1. To identify and analyse the threat of money laundering (ML) and terrorism financing (TF) in the Non-Bank EM and EW sector;
2. To identify the vulnerabilities and consequences of money laundering and terrorism financing through the Non-Bank EM and EW sector; and
3. To analyse the key risks of money laundering and terrorism financing.

Non-Bank EM and EW Sectoral Risk Assessment (SRA) mapped four key risk areas, namely service user, location, product and delivery channel with the risk factors covering threats, vulnerabilities and consequences. The analysis method refers to the risk assessment published by the Financial Action Task Force (FATF). Based on the results of the assessment, the level of ML and TF risks in Non-Bank EM and EW sector was determined as follows:

1. **Jakarta** was identified as a **high-risk** region in terms of ML and TF activity in the Non-Bank EM and EW, followed by **West Java, North Sumatra** and **Bengkulu** (**medium risk**). All other provinces in Indonesia were categorised as **low risk**.
2. In terms of customer profile, **PEPs** and **Private Sector Employees** were considered **high risk** in terms of ML and TF activity in the Non-Bank EM and EW sector, followed by **students, entrepreneurs** and **professionals** (**medium risk**). All other customer profiles were identified as **low risk**.
3. **Cash top-ups** were the product feature identified as **high risk** in terms of ML and TF activity in the Non-Bank EM and EW sector, followed by **noncash top-ups** that were categorised as **medium risk**. All other products were considered **low risk**.
4. **Offline merchants** were identified as a **high-risk** delivery channel in terms of ML and TF activity in the Non-Bank EM and EW sector, followed by **DFS agents** (**medium risk**). Bank transfers, debit cards, outlets and online merchants were considered **low risk**.
5. Unregistered EM were identified as **low risk** considering the low risk of ML and TF in general, coupled with prevailing risk mitigation measures, such as restrictions on floats and transaction value. Furthermore, Unregistered Non-Bank EM and EW are proscribed from transferring funds.

In terms of ML and TF risk mitigation in the Non-Bank EM and EW sector, Bank Indonesia has issued regulations and guidelines as well as implemented on-site and off-site supervision. In addition, Bank Indonesia actively engages in domestic and international cooperation. Moreover, Bank Indonesia has also provided socialisation and education activities targeting Non-Bank EM and EW and the public in order to build awareness around the prevention and eradication of ML and TF.

1 LITERATURE REVIEW

A. Legal Basis

Bank Indonesia has been designated a Supervisory and Regulatory Body (LPP) for Electronic Money and Electronic Wallets in accordance with Act No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering. E-money is regulated pursuant to Bank Indonesia Regulation (PBI) No. 20/6/PBI/2018 concerning Electronic Money. Furthermore, e-wallets are regulated in accordance with Bank Indonesia Regulation (PBI) No. 18/40/PBI/2016 regarding Payment Transaction Processing. The provisions include:

1. The principles and scope of e-money issuers;
2. Licensing and approval of e-money issuers;
3. Risk management implementation;
4. Information system security standards;
5. Anti-money laundering and counter-terrorism financing implementation;
6. Implementation of consumer protection principles;
7. Digital financial services (DFS) agents;
8. Reporting and oversight; and
9. Sanctions

B. Characteristics of Electronic Money and Electronic Wallets in Indonesia

1. Definition

Electronic Money[14] is a payment instrument characterised by the following:

a. Issued based on the value of currency deposited in advance with the issuer;
b. The value of currency stored electronically on a server or chip; and
c. The value of e-money managed by an issuer is not considered a deposit in accordance with prevailing banking laws.

Issuers are entities that issue e-money, while the value of e-money is the value of currency stored electronically on a server or chip that can be moved for the purpose of payment transactions and/or fund transfers. All e-money issuers are required to obtain an operating licence from Bank Indonesia. Non-bank institutions[15] applying for an operating licence as an e-money issuer are required to meet minimum paid-up capital requirements of Rp3 billion and then adjust the level of paid-up capital based on the position of the float[16]. Furthermore, the shareholder composition of e-money issuers must contain at least 51% of Indonesian residents and/or a legal entity incorporated in Indonesia. The operating licence for e-money issuers issued by Bank Indonesia is valid for five years and may be extended upon request. E-money and e-wallet issuers are required to implement anti-money laundering and counter-terrorism financing as well as consumer protection principles.

[14] Article 1, paragraph (3) of Bank Indonesia Regulation (PBI) No. 20/6/PBI/2018 concerning Electronic Money.

[15] In accordance with Article 1, paragraph (2) of Bank Indonesia Regulation (PBI) No. 20/6/PBI/2018 concerning Electronic Money, nonbank institutions are Non-Bank business entities incorporated in Indonesia.

[16] Articles 9 and 50 of Bank Indonesia Regulation (PBI) No. 20/6/PBI/2018 concerning Electronic Money.

Issuers are required to process payment transactions domestically using e-money issued and transacted in the territory of the Republic of Indonesia. E-money and e-wallets issued outside the territory of the Republic of Indonesia may only be transacted inside the territory of the Republic of Indonesia using payment channels connected to the National Payment Gateway (NPG). Each party engaged in such transactions is required to cooperate with an authorised payment system service provider, namely a BUKU 4 bank[17], connected to the National Payment Gateway (NPG). Bank Indonesia is authorised to appraise the competencies and compliance of the controlling shareholders, directors and members of the Board of Commissioners of non-bank institutions.

2. Product and Services

Electronic money has the following distinguishing characteristics:

a. Based on scope, e-money is categorised as closed-loop[18] and open-loop[19];

b. Based on the storage media, e-money is categorised as server-based[20] and chip-based[21]; and

c. based on recording user identity data, e-money is categorised as unregistered[22] and registered[23].

Any issuer of open-loop or closed-loop electronic money with a float of at least Rp1 billion is required to obtain a licence from Bank Indonesia. The maximum value of unregistered electronic money and unregistered electronic money in an electronic wallet is Rp2 million and Rp10 million for registered electronic money and registered electronic money in an electronic wallet. In one month, the maximum transaction value of electronic money and electronic money in an electronic wallet is Rp 20 million based on incoming transactions.

3. Issuers

As of 31st March 2019, Bank Indonesia had licensed 25 non-bank institutions as Non-Bank Electronic Money Issuers and two Non-Bank Electronic Wallet Issuers. Based on the distribution data, all e-money and e-wallet issuers were located in Jakarta. According to Bank Indonesia data, all Non-Bank institutions licensed as Non-Bank e-wallet issuers were also licensed as Non-Bank money issuers, therefore, an integrated risk assessment of both instruments was conducted.

[17] In accordance with Bank Indonesia Regulation (PBI) No. 14/26/PBI/2012 concerning Operating Activities and Branch Network based on Core Capital, a BUKU 4 bank is required to maintain core capital exceeding Rp30 trillion.

[18] In accordance with Article 3, paragraph (1) of Bank Indonesia Regulation (PBI) No. 20/6/PBI/2018 concerning Electronic Money, closed loop means electronic money can only be used as a payment instrument to the goods and/or services provider (merchant) also acting as issuer of that e-money.

[19] In accordance with Article 3, paragraph (1) of Bank Indonesia Regulation (PBI) No. 20/6/PBI/2018 concerning Electronic Money, open loop means electronic money can be used as a payment instrument for goods and/or services providers that are not issuers of the e-money.

[20] In accordance with Article 3, paragraph (2) of Bank Indonesia Regulation (PBI) No. 20/6/PBI/2018 concerning Electronic Money, server-based electronic money uses a server-based storage media.

[21] In accordance with Article 3, paragraph (2) of Bank Indonesia Regulation (PBI) No. 20/6/PBI/2018 concerning Electronic Money, chip-based electronic money uses a chip-based storage media.

[22] In accordance with Article 3, paragraph (2) of Bank Indonesia Regulation (PBI) No. 20/6/PBI/2018 concerning Electronic Money, unregistered means the issuer does not register or record user identification data.

[23] In accordance with Article 3, paragraph (2) of Bank Indonesia Regulation (PBI) No. 20/6/PBI/2018 concerning Electronic Money, registered means the issuer registers and records user identification data.

2 KEY RISK IN THE NON-BANK ELECTRONIC MONEY AND ELECTRONIC WALLET SECTOR

A. ML Risk Landscape in the Non-Bank Electronic Money and Electronic Wallet Sector

The modus operandi of money laundering in Indonesia has become increasingly complex and diverse over time, with institutions outside the financial system potentially being targeted. Based on the results of a National Risk Assessment (NRA) of ML and TF, the predicate offences are dominated by narcotics, corruption and banking crime. As payment instruments, e-money and e-wallets are susceptible to exploitation for money-laundering purposes, although no significant ML cases have been uncovered.

B. TF Risk Landscape in the Non-Bank Electronic Money and Electronic Wallet Sector

No TF cases using e-money or e-wallets were uncovered during the research period.

C. ML and TF Risk Assessment in the Non-Bank Electronic Money and Electronic Wallet Sector

1. ML and TF Risk by Region

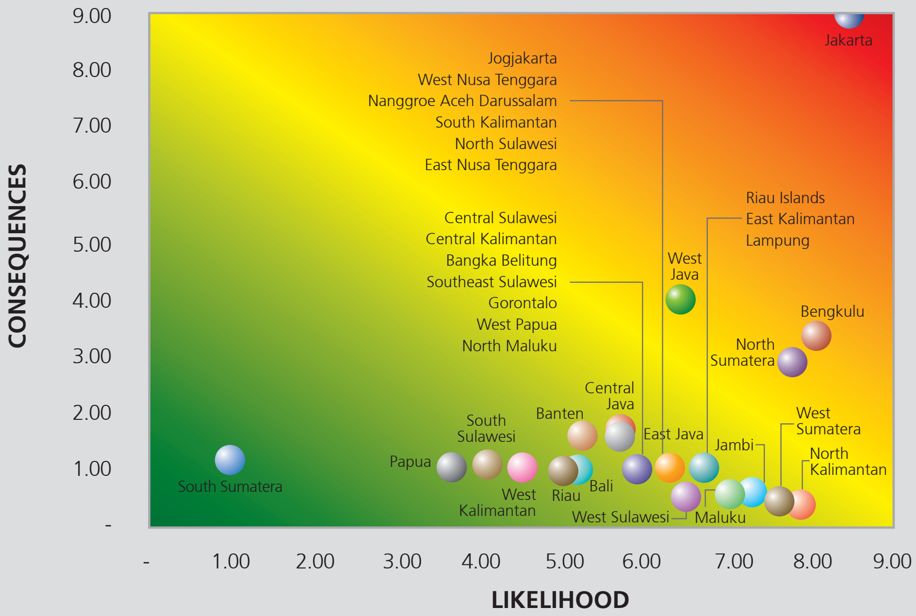
ML and TF risks were assessed by region in order to investigate which provinces were most at risk to ML and TF cases in the Non-Bank Electronic Money and Electronic Wallet sector. The regional risk assessment was conducted in all Indonesian provinces where customers of non-bank e-money and e-wallet issuers were located. Risk was assessed as a function of threat, vulnerability and consequence in each respective province, with the three aspects measured based on predetermined risk factors.

The level of risk by region was calculated as a function of multiplying the likelihood by the consequences in each respective province, where the likelihood is the sum of the threat and vulnerability. The following heat map illustrates ML and TF risks in the non-bank e-money and e-wallet sector by region expressed as a function of threat, vulnerability and consequence (Figure 2.3.1):

According to the heat map of risk presented below, **Jakarta** was identified as **high risk** in terms of ML and TF activity in the non-bank e-money and e-wallet sector. On the other hand, the **medium-risk** regions were **Bengkulu, West Java** and **North Sumatra**, while all other provinces were deemed low risk.

The values for threat and consequence were highest in Jakarta, coupled with a low level of vulnerability. Jakarta's position on the x-axis of the heat map revealed a higher likelihood than other regions. Furthermore, the position on the y-axis showed that the consequences of ML and TF in the non-bank e-money and e-wallet sector in Jakarta were also highest compared with other regions.

Figure 2.3.1.
Risk by Region



The provinces of Bengkulu, West Java and North Sumatra were considered at medium risk to ML and TF incidences in the non-bank e-money and e-wallet sector. In terms of threat, Bengkulu was identified as low despite one Suspicious Financial Transaction Report (STR) submitted. Notwithstanding, the number of customers in Bengkulu was also very low, the lowest of the four other provinces. For the consequences, Bengkulu received a medium score. Regarding vulnerability, Bengkulu was identified as highly vulnerable because of constraints in terms of identifying and reporting suspicious financial transactions as well as weak identification of regional risks, except Jakarta.

West Java received medium scores for threat, vulnerability and consequence. The medium values for threat and consequence were due to West Java's endowment as a province with the largest user base for electronic money after Jakarta in terms of total customers and transaction value. Concerning vulnerability, the non-bank e-money and e-wallet sector in West Java was considered competent in terms of identifying and reporting suspicious financial transactions.

Sumatra province was identified as a region with medium scores for vulnerability and threat. The threat in Sumatra was considered medium due to the high number of customers and one existing Suspicious Financial Transaction Report (STR). Nonetheless, the consequences were deemed low due to a lower transaction value compared to Jakarta and West Java.

2. ML and TF Risk by Customer Profile

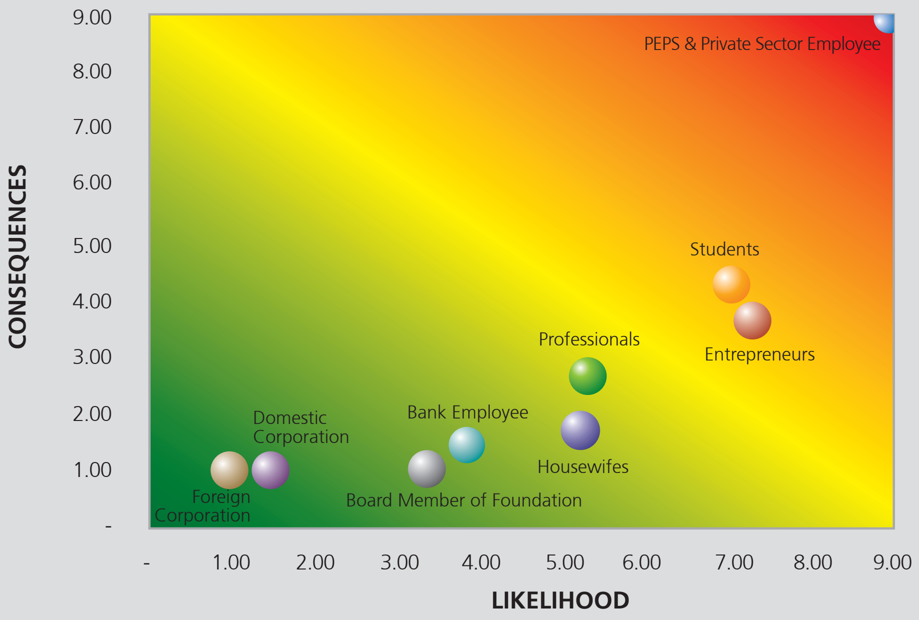
ML and TF risk were also assessed based on customer profile in order to investigate which profiles (professions) were most at risk to ML and TF in the non-bank e-money and e-wallet sector. The types of customer profile assessed were those identified in the NRA as high and medium risk of committing ML and TF. The risk assessment based on customer profile in the non-bank e-money and e-wallet sector faced the following limitations:

1) The requirement for e-money and e-wallet issuers to administrate information concerning services users in accordance with Article 51 of Bank Indonesia's Anti-Money Laundering and Countering Terrorism Financing (AML/CFT) Regulation[24].
2) The questionnaire did not explicitly measure Politically Exposed Persons (PEP) because PEPs are directly categorised as high-risk customers.

The level of risk based on customer profile was calculated as a function of multiplying the likelihood by the consequences for each respective profile, where the likelihood is the sum of the threat and vulnerability. The following heat map illustrates ML and TF risks in the Non-Bank e-money and e-wallet sector by customer profile expressed as a function of threat, vulnerability and consequence (Figure 2.3.2):

According to the heat map of risk presented below, the customer profile considered **high** risk in terms of ML and TF incidences in the Non-Bank e-money and e-wallet sector was **Private Sector Employees,** while the **medium-risk** customer profiles were **Entrepreneurs** and **Professionals** and all other customer profiles were deemed low risk.

Figure 2.3.2.
Risk by Customer Profile



[24] Issuers/providers are required to maintain service user data for a minimum period of five years: (i) after the business relationship or transaction with the service user has ended; or (ii) if discrepancies between the transaction and risk profile of the service user are discovered.

Private Sector Employees had the highest threat and consequence readings of all customer profiles, with a medium vulnerability score. This was because Private Sector Employees dominated the number of transactions and customers compared to all other customer profiles, and also due to competence in the non-bank e-money and e-wallet sector to identify and report suspicious financial transactions.

The position of Private Sector Employees on the x-axis of the heat map demonstrated a higher likelihood than the other profiles. Meanwhile, the position of Private Sector Employees on the y-axis of the heat map showed that the consequences of ML and TF in the non-bank e-money and e-wallet sector by Private Sector Employees were higher than the other customer profiles.

In accordance with Article 34 of Bank Indonesia Regulation (PBI) No. 19/10/PBI/2017 concerning Anti-Money Laundering and Countering Terrorism Financing (AML/CFT) for Payment System Service Providers and KUPVA BB, and in reference to FATF Guidance on Politically Exposed Persons that states PEPs are particularly vulnerable to money laundering, prospective service users, service users and beneficial owners that are categorised as PEPs were also considered high-risk customer profiles.

Entrepreneurs and Professionals were considered medium risk in terms of ML and TF incidences in the non-bank e-money and e-wallet sector. Regarding the threat, consequences and vulnerability, Entrepreneurs received medium scores. Meanwhile, Professionals were high risk in terms of vulnerability, yet low in terms of threat and consequences because e-money and e-wallet issuers sub-optimally identify and report suspicious financial transactions.

3. ML and TF Risk by Product

ML and TF risk were assessed on a product-by-product basis in order to explore which products were most at risk to ML and TF cases in Non-Bank e-money and e-wallet sector. The ML and TF risks were assessed based on registered e-money issuers because:

1) the maximum value of e-money stored by an unregistered e-money is Rp2 million, which is thus considered low risk;
2) the customer verification process to register e-money and e-wallets requires a national ID card and mobile telephone number[25].

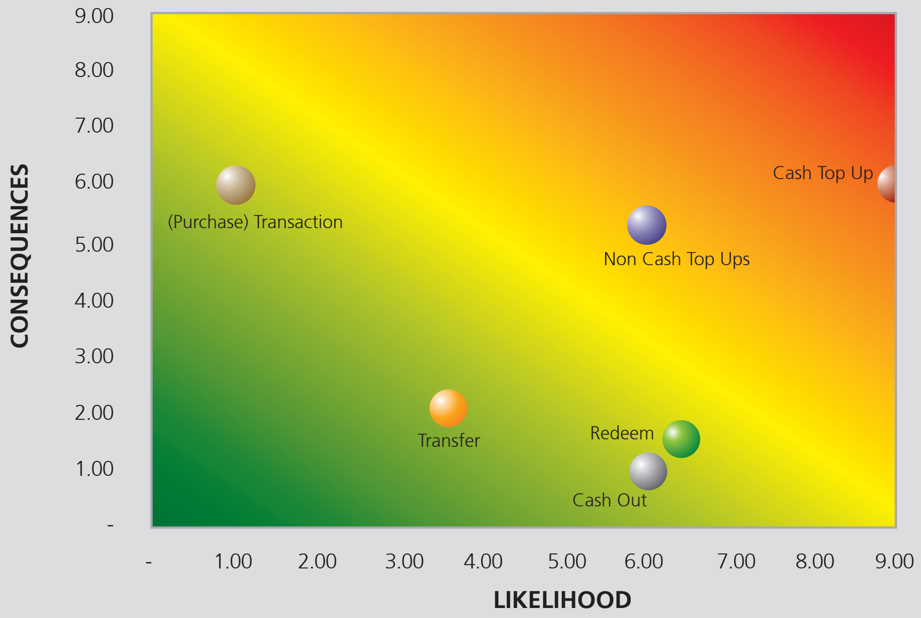
The level of risk based on product was calculated as a function of multiplying the likelihood by the consequences for each respective product, where the likelihood is the sum of the threat and vulnerability. The following heat map illustrates ML and TF risks in the non-bank e-money and e-wallet sector by product expressed as a function of threat, vulnerability and consequence (Figure 2.3.3):

According to the heat map of risk presented below, the product considered **high risk** in terms of ML and TF incidences in the non-bank e-money and e-wallet sector was **Cash Top Ups,** followed by **Noncash Top Ups** that were identified as a **medium-risk** product, while all other products were deemed low risk.

Cash Top Ups received a medium vulnerability score and the highest consequence level amongst all other products. The position of Cash Top Ups on the x-axis of the heat map demonstrated a higher likelihood than the other products. Meanwhile, the position on the y-axis of the

[25] In accordance with Minister of Communications and Informatica Regulation No.12 of 2016 concerning the Registration of Communication Services Subscribers, cellular telephone users are required to register using a valid ID in order to access communications services.

Figure 2.3.3.
Risk by Product



heat map showed that the consequences of ML and TF in the non-bank e-money and e-wallet sector using Cash Top Ups was highest compared with the other products.

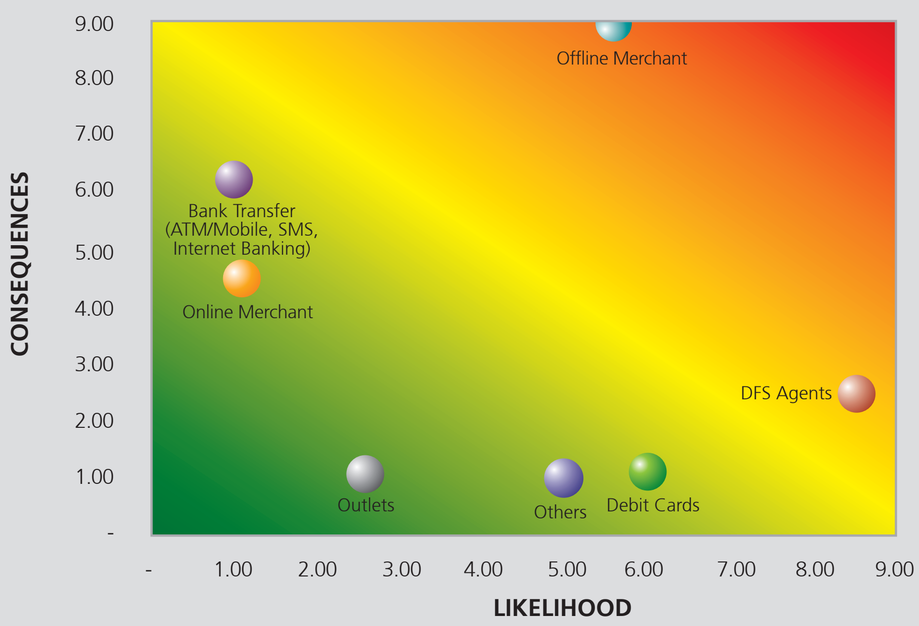
Noncash Top Ups were considered a medium-risk product in terms of ML and TF in the non-bank e-money and e-wallet sector. The vulnerability level of Noncash Top Ups was deemed high, yet with a low consequence score due to a low transaction value compared with other e-money and e-wallet products, such as Cash Top Ups and (Purchase) Transactions.

4. ML and TF Risk by Delivery Channel

ML and TF risk were assessed based on delivery channel in order to explore which delivery channels were most at risk to cases of ML and TF in the non-bank e-money and e-wallet sector. As the object of the risk assessment, the delivery channels were categorised into six groups; DFS Agents, Debit Cards, Outlets, Offline Merchants, Online Merchants and Bank Transfers. The remaining delivery channels (including websites and vending machines) were grouped into the Others category. Risk was assessed as a function of threat, vulnerability and consequence of each respective delivery channel, with the three aspects measured based on predetermined risk factors.

The level of risk was calculated as a function of multiplying the likelihood by the consequences for each respective delivery channel, where the likelihood is the sum of the threat and vulnerability. The following heat map illustrates ML and TF risks in the non-bank e-money and e-wallet sector by delivery channel expressed as a function of threat, vulnerability and consequence (Figure 2.3.4):

Figure 2.3.4.
Risk by Delivery Channel



According to the heat map of risk presented above, the delivery channel considered **high risk** in terms of ML and TF incidences in the non-bank e-money and e-wallet sector was **Offline Merchants,** followed by **DFS Agents** that were identified as a **medium-risk** delivery channel, while all other delivery channels were deemed **low risk**.

Offline Merchants received a low vulnerability score yet the highest consequence level amongst all delivery channels. The position of Offline Merchants on the x-axis of the heat map demonstrated a higher likelihood than the other delivery channels. Meanwhile, the position on the y-axis of the heat map showed that the consequences of ML and TF in the non-bank e-money and e-wallet sector through Offline Merchants was highest compared with the other delivery channels.

DFS Agents were considered a medium-risk delivery channel in terms of ML and TF incidences in the non-bank e-money and e-wallet sector. The consequence level of DFS Agents was deemed low because although the transaction value processed through DFS Agents was high, the value was low in comparison to other delivery channels, such as Offline Merchants, Bank Transfers and Online Merchants.

3 RISK MITIGATION

A. Risk Mitigation: Institutional Aspects

1. Non-Bank e-Money and e-Wallet Issuers operating in Indonesia are required to obtain a licence from Bank Indonesia.
2. Non-Bank e-Money issuers are not permitted to undertake corporate actions that change the structure of the controlling shareholders for five years from the date when the licence is first issued, except under certain conditions with approval from Bank Indonesia.
3. Bank Indonesia will assess the competence and compliance of controlling shareholders, directors and members of the board of commissioners of Non-Bank Institutions licensed as e-Money Issuers. The appraisal aims to ensure integrity, financial reputation, financial viability and competence.
4. Non-Bank e-Money and e-Wallet Issuers are required to maintain a minimum of a 51% local shareholding.
5. The licence issued by Bank Indonesia to e-Money Issuers is valid for five years and may be extended upon request.
6. e-Money Issuers seeking to operate as DFS Providers are required to first obtain approval from Bank Indonesia. Providers of digital financial services (DFS) through cooperation with DFS Agents may be business entities incorporated in Indonesia and/or individuals. Digital financial services through individual DFS Agents may only be provided by DFS banks.

B. Risk Mitigation: Product Features

1. Non-Bank e-Money and e-Wallet Issuers are prohibited from using virtual currency to receive, use, link and/or process electronic money and electronic wallet payment transactions.
2. The maximum value of unregistered electronic money and unregistered electronic money in an electronic wallet is Rp2 million and Rp10 million for registered electronic money and registered electronic money in an electronic wallet. In one month, the maximum transaction value of electronic money and electronic money in an electronic wallet is Rp 20 million, based on incoming transactions.
3. Unregistered electronic money cannot be used for funds transfers.

C. Risk Mitigation: Operational Aspects

1. The Directors and Board of Commissioners are required to supervise AML/CFT program implementation.
2. e-Money and e-Wallet Issuers are required to implement identification and verification; manage the data, information and documents; as well as report to the authorities.
3. Non-Bank e-Money and e-Wallet Issuers are required to implement more rigorous identification procedures for high-risk Prospective Service Users, Service Users and Beneficial Owners.
4. Non-Bank e-Money and e-Wallet Issuers are required to identify and report suspicious financial transactions to INTRAC.

5. Non-Bank e-Money and e-Wallet Issuers are required to identify, assess, control and mitigate the risks.
6. Non-Bank e-Money and e-Wallet Issuers are required to implement employee screening, monitor employee profiles and provide capacity building to employees.
7. Non-Bank e-Money and e-Wallet Issuers are required to apply internal controls, for example a periodic independent audit, to test AML/CFT compliance and implementation.
8. Non-Bank e-Money and e-Wallet Issuers are required to administrate, update and check the List of Suspected Terrorist Organisations and Individuals (DTTOT) and the list of financing of proliferation of weapons of mass destruction against customer information.
9. Registered Non-Bank e-Money and e-Wallet Issuers are required to apply e-KYC principles by ensuring that all customers register their mobile phone number (in accordance with prevailing Minister of Communication and Information Technology Regulations), while also sending a scanned ID card and self-portrait together with the corresponding ID card in order to prevent unauthorised use of ID cards not matching the customer profile.

D. Risk Mitigation: Oversight

1. Bank Indonesia implements on-site and off-site risk-based supervision of AML/CFT implementation by Non-Bank e-Money and e-Wallet Issuers.
2. Bank Indonesia implements thematic supervision of Non-Bank e-Money and e-Wallet Issuers.
3. Bank Indonesia may appoint a third party to inspect a Non-Bank e-Money and e-Wallet Issuer on behalf of Bank Indonesia.
4. For oversight by Bank Indonesia, Non-Bank e-Money and e-Wallet Issuers are required to identify, administrate and update the data on beneficial owners, while ensuring the availability of such data to Bank Indonesia for supervision purposes.

4 CONCLUSION

Based on the results of the sectoral statistical analysis, the level of ML and TF risk in the non-bank e-money and e-wallet sector, in terms of location, customer profile, product and delivery channel, was determined as follows (Table 2.3.1):

1. **Jakarta** was a **high-risk** region in terms of ML and TF activity in the non-bank e-money and e-wallet sector, followed by **West Java, North Sumatra** and **Bengkulu** (**medium risk**). All other provinces in Indonesia were categorised as **low risk**.
2. In terms of customer profile, **PEPs** and **Private Sector Employees** were considered **high risk** in terms of ML and TF activity in the non-bank e-money and e-wallet sector, followed by **students, entrepreneurs** and **professionals** (**medium risk**). All other customer profiles were **low risk**.
3. **Cash top-ups** were the product feature identified as **high risk** in terms of ML and TF activity in the non-bank e-money and e-wallet sector, followed by **noncash top-ups** that were **medium risk**. All other products were **low risk**.
4. **Offline merchants** were a **high-risk** delivery channel in terms of ML and TF activity in the non-bank e-money and e-wallet sector, followed by **DFS agents** (**medium risk**). Bank transfers, debit cards, outlets and online merchants were considered **low risk**.
5. Unregistered EM were **low risk** considering the low risk of ML and TF, coupled with prevailing risk mitigation measures, such as restrictions on floats and transaction value. Furthermore, unregistered non-bank e-money and e-wallet sector is prohibited from transferring funds.

Table 2.3.1.
SRA Results for Non-Bank e-Money and e-Wallet Issuers

SRA Results for Non-Bank e-Money and e-Wallet Issuers

Risk	Location	Customer	Product	Delivery Channel
High	Jakarta	PEP and Private Sector Employee	Cash Top Up	Offline merchant
Medium	West Java, Bengkulu, North Sumatra	Student, Entrepreneur and Professional	Noncash Top Up	DFS Agent
Low	Others	Bank Employee, Housewife, Board Member of Foundation, Corporation	Transfer, Cash Out, Redeem, Purchase Transaction	Bank Transfer, Debit Card, Outlet, Online Merchant

Non-Bank Issuers of Card Based Payment Instrument

Executive Summary

In 2019, the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC) in conjunction with relevant government ministries/institutions updated the National Risk Assessment (NRA 2015 Updated). As a follow-up risk-mitigation action against money laundering and terrorism financing at Non-Bank Issuers of Card-Based Payment Services (Non-Bank CBPS), a sectoral risk assessment has been conducted. The Sectoral Risk Assessment (SRA) was compiled with the following objectives:

1. To identify and analyse the threat of money laundering (ML) and terrorism financing (TF) in the Non-Bank CBPS sector;
2. To identify than vulnerabilities and consequences of money laundering and terrorism financing through the Non-Bank CBPS sector; and
3. To analyse the key risks of money laundering and terrorism financing.

The Non-Bank CBPS SRA mapped four key risk areas, namely service user, location, product and delivery channel with the risk factors covering threats, vulnerabilities and consequences. The analysis method refered to the risk assessment published by the Financial Action Task Force (FATF). Based on the results of the assessment, the level of ML and TF risks in the Non-Bank CBPS sector was determined as follows:

1. **Jakarta** was identified as a **high-risk** region in terms of ML and TF activity in the Non-Bank CBPS sector, followed by **Banten** and **West Java** (**medium risk**). All other provinces in Indonesia were categorised as **low risk**.
2. In terms of customer profile, **PEPs** and **Private Sector Employees** were **high risk** in terms of ML and TF activity in the non-bank CBPS sector. All other customer profiles were identified as **low risk**.
3. **Retail** was the product feature identified as **high risk** in terms of ML and TF activity in the Non-Bank CBPS sector. On the other hand, cash withdrawals were **low risk**.
4. **Offline merchants** were identified as a **high-risk** delivery channel in terms of ML and TF activity in the Non-Bank CBPS sector. ATM (cash withdrawals) and online merchants were **low risk**.

In terms of ML and TF risk mitigation in the Non-Bank CBPS sector, Bank Indonesia has issued regulations and guidelines as well as implemented on-site and off-site supervision. In addition, Bank Indonesia actively engages in domestic and international cooperation. Moreover, Bank Indonesia has also provided socialisation and education activities targeting Non-Bank CBPS Issuers and the public in order to build awareness around the prevention and eradication of ML and TF.

1 LITERATURE REVIEW

A. Legal Basis

Bank Indonesia has been designated a Supervisory and Regulatory Body (LPP) for card-based payment instrument activity in accordance with Act No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering. In terms of AML/CFT policies and supervision, Bank Indonesia has jurisdiction over Non-Bank CBPS Issuers as non-bank legal entities providing card-based payment instrument services.

Regulatory provisions regarding Non-Bank CBPS Issuer activity are contained within Bank Indonesia Regulation (PBI) No.11/11/PBI/2019 as an amendment to Bank Indonesia Regulation (PBI) No.14/2/PBI/2012 concerning Card-Based Payment Instrument Activity, dated 6th January 2012 as follows:

1. Interest rate cap for Credit Cards as determined by Bank Indonesia through a Bank Indonesia Circular Letter;
2. Credit card requirements, including minimum age, minimum income, credit limit and number of Issuers permitted to offer Credit Card facilities, which are contained in a corresponding Bank Indonesia Circular Letter;
3. Prudential principles and consumer protection, including standardised methods to calculate credit card interest rates, costs and fines as well as information disclosure requirements to the cardholders;
4. Third-party outsourcing with reference to the Bank Indonesia Regulation concerning Outsourcing, particularly in terms of collecting credit card debt;
5. Enhancing transaction security for payment instruments through mandatory transaction alerts/notifications for the cardholders;
6. Interoperability requirements;
7. Bank Indonesia's authority to license and impose sanctions on CBPS Issuers.

B. Characteristics of Card Based Payment Instrument Activity in Indonesia

1. Definition

Card-based payment services (CBPS) instruments include credit cards, automated teller machine (ATM) cards and/or debit cards[26].

A credit card is a card-based payment services (CBPS) instrument used to pay a merchant for goods and services and/or to make cash withdrawals, with the cardholders' payment obligations initially met by the acquirer or issuer before the cardholder is required to make a payment by an agreed date with the balance to be repaid in full each month (charge card) or repaid in instalments[27].

An ATM card is a card-based payment services (CBPS) instrument used to withdraw cash and/or move funds, where the cardholder's obligations are settled and deducted directly from the cardholder's deposit account at a bank or Non-

[26] Article 1, paragraph (3) of Bank Indonesia Regulation (PBI) No. 14/2/PBI/2012 concerning Card-Based Payment Instruments.

[27] Article 1, paragraph (4) of Bank Indonesia Regulation (PBI) No. 14/2/PBI/2012 concerning Card-Based Payment Instruments.

Bank financial institution authorised to store funds in accordance with prevailing laws and regulations[28].

A debit card is a card-based payment services (CBPS) instrument used to pay a merchant for goods and services (retail), where the cardholder's obligations are settled and deducted directly from the cardholder's deposit account at a bank or non-bank financial institution authorised to store funds in accordance with prevailing laws and regulations[29].

2. **Issuers**

   As of 31st March 2019, Bank Indonesia had licensed two non-bank financial institutions as Non-Bank Issuers of Card-Based Payment Services Instruments.

[28] Article 1, paragraph (5) of Bank Indonesia Regulation (PBI) No. 14/2/PBI/2012 concerning Card-Based Payment Instruments.

[29] Article 1, paragraph (6) of Bank Indonesia Regulation (PBI) No. 14/2/PBI/2012 concerning Card-Based Payment Instruments.

2 KEY RISK IN THE NON-BANK CBPS SECTOR

A. ML Risk Landscape in the Non-Bank CBPS Sector

The modus operandi of money laundering in Indonesia has become increasingly complex and diverse over time using institutions outside of the banking system. Based on the results of a National Risk Assessment (NRA) of ML and TF, the predicate offences of most money laundering cases in Indonesia are dominated by narcotics, corruption and banking crime. Non-Bank card-based payment instruments can be used as a media to launder money despite no significant ML cases using non-bank card-based payment instruments being prosecuted thus far.

B. TF Risk Landscape in the Non-Bank CBPS Sector

No cases of terrorism financing using non-bank card-based payment instruments were prosecuted during the research period.

C. ML and TF Risk Assessment in the Non-Bank CBPS Sector

1. ML and TF Risk by Region

ML and TF risks were assessed by region in order to investigate which provinces were most at risk to ML and TF activity in the Non-Bank CBPS sector. The objects of the regional risk assessment were identified as **medium** and **high-risk** provinces in terms of ML and TF incidences in Indonesia based on the National Risk Assessment (NRA), where Non-Bank CBPS issuers are located. Risk was assessed as a function of threat, vulnerability and consequence in each respective province, with the three aspects measured based on predetermined risk factors.

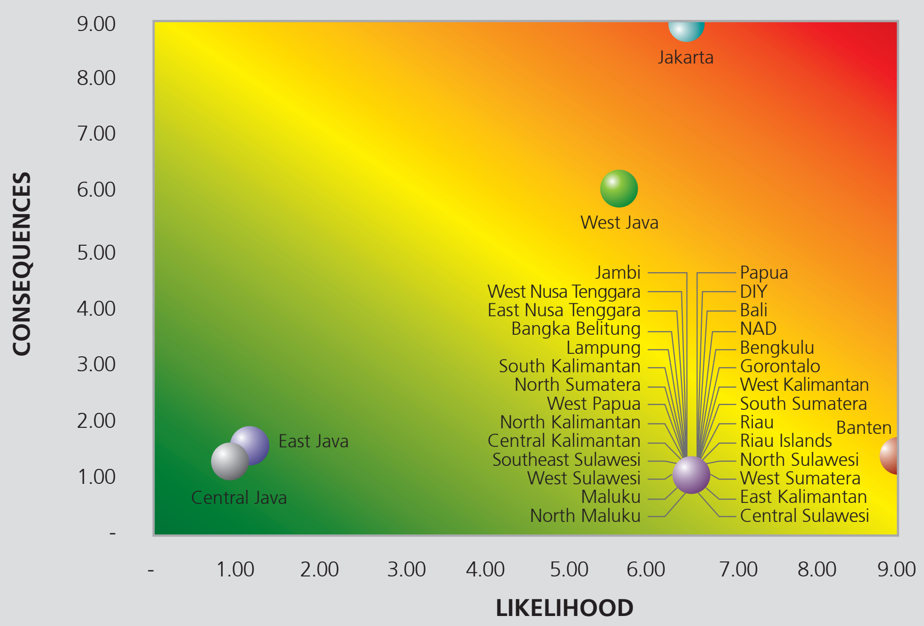
The level of risk by region was calculated as a function of multiplying the likelihood by the consequences in each respective province, where the likelihood is the sum of the threat and vulnerability. The following heat map illustrates ML and TF risks in the Non-Bank CBPS sector by region expressed as a function of threat, vulnerability and consequence (Figure 2.4.1):

According to the heat map of risk presented below, **Jakarta** was considered high risk in terms of ML and TF in the Non-Bank CBPS sector. On the other hand, the **medium-risk** regions were **Banten** and **West Java,** while all other provinces were deemed low risk.

The values for threat and consequence were highest in Jakarta, coupled with a low vulnerability reading. Jakarta's position on the x-axis of the heat map revealed a higher likelihood than other regions. Furthermore, the position on the y-axis shows that the consequences of ML and TF in the Non-Bank CBPS sector in Jakarta were also highest compared with other regions.

The provinces of Banten and West Java were considered medium risk to ML and TF incidences in the Non-Bank CBPS sector. In terms of threat and consequences, Banten was identified as medium risk. Meanwhile, West Java received a high threat value and medium consequence score. Such conditions were due to the significantly lower level of transactions using card-based payment instruments compared to Jakarta, which was identified as a high consequence region.

Figure 2.4.1.
Risk by Region



2. ML and TF Risk by Customer Profile

ML and TF risk were also assessed based on customer profile in order to investigate which profiles (professions) were most at risk to ML and TF in the Non-Bank CBPS sector. The types of customer profile assessed were those identified in the **NRA** as **high** and **medium** risk of committing ML and TF.

The risk assessment based on customer profile in the Non-Bank CBPS sector faced the following limitations:

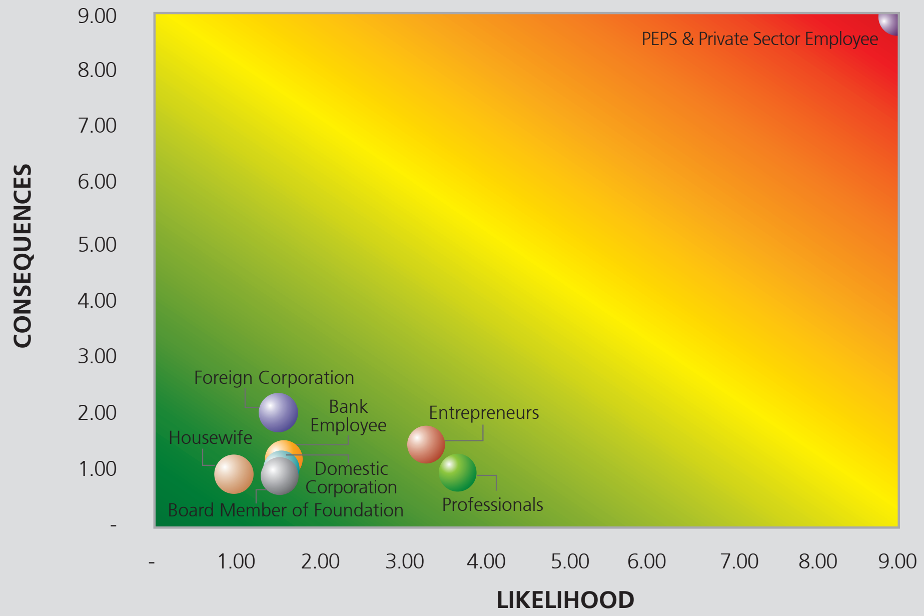
a. The requirement for Non-Bank CBPS issuers to administrate information concerning services users in accordance with Article 51, paragraph (1) of Bank Indonesia Regulation (PBI) No. 19/10/PBI/2017 regarding Anti-Money Laundering and Countering Terrorism Financing (AML/CFT) for Payment System Service Providers and KUPVA BB.

b. The prevailing characteristics of customers in the Non-Bank CBPS sector, most of whom already hold a card-based payment instrument issued by the banking industry and maintain a bank savings account. Consequently, there is overlapping Customer Due Diligence implemented by the Non-Bank CBPS sector and the banking industry.

c. The questionnaire did not explicitly measure Politically Exposed Persons (PEP) because PEPs are directly categorised as high-risk customers.

The level of risk based on customer profile was calculated as a function of multiplying the likelihood by the consequences for each respective customer profile, where the likelihood is the sum of the threat and vulnerability. The following heat map illustrates ML and TF risks in the Non-Bank CBPS sector by customer profile expressed as a function of threat, vulnerability and consequence (Figure 2.4.2):

Figure 2.4.2.
Risk by Customer Profile



According to the heat map of risk presented above, the customer profile identified as **high risk** in terms of ML and TF activity in the Non-Bank CBPS sector was Private Sector Employees, while all other customer profiles were deemed low risk.

Private Sector Employees had the highest threat, consequence and vulnerability scores. The position of Private Sector Employees on the x-axis of the heat map demonstrated a higher likelihood than the other profiles. Meanwhile, the position of Private Sector Employees on the y-axis of the heat map showed that the consequences of ML and TF in the Non-Bank CBPS sector by Private Sector Employees was highest compared with other customer profiles.

In accordance with Article 34 of Bank Indonesia Regulation (PBI) No. 19/10/PBI/2017 concerning Anti-Money Laundering and Countering Terrorism Financing (AML/CFT) for Payment System Service Providers and KUPVA BB, and in reference to FATF Guidance on Politically Exposed Persons that states PEPs are particularly vulnerable to money laundering, prospective service users, service users and beneficial owners that are categorised as PEPs were also considered high-risk customer profiles.

3. ML and TF Risk by Product

ML and TF risk were assessed on a product-by-product basis in order to explore which products were most at risk to ML and TF cases in the Non-Bank CBPS sector. The product-based risk assessment for the Non-Bank CBPS sector faced the following limitations:

a. In accordance with Bank Indonesia's authority, AML/CFT policy and supervision only extends to card-based payment instruments issued by Non-Bank Issuers. As of March 2019, only two Non-Bank CBPS issuers were registered in Indonesia.

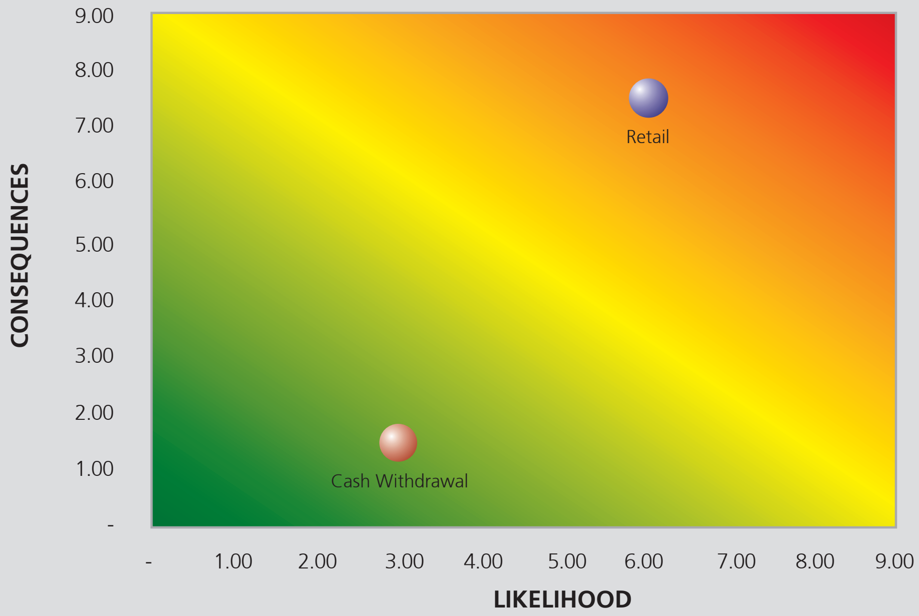
b. The object of the assessment was limited to credit cards because Non-Bank CBPS issuers in Indonesia are restricted from issuing ATM Cards or Debit Cards.

The level of risk based on product was calculated as a function of multiplying the likelihood by the consequences for each respective product, where the likelihood is the sum of the threat and vulnerability. The following heat map illustrates ML and TF risks in the Non-Bank CBPS sector by product expressed as a function of threat, vulnerability and consequence (Figure 2.4.3):

Retail received medium threat and vulnerability values with a high consequence score. Cash, on the other hand, received low scores for threat, vulnerability and consequence. The position of retail on the x-axis of the heat map demonstrated a higher likelihood than the cash product. Meanwhile, the position on the y-axis of the heat map showed that the consequences of ML and TF in the Non-Bank CBPS sector through retail products were higher than cash products.

Cash products received low values for threat, vulnerability and consequence because in terms of total customers, transaction value was lower than retail products. Furthermore, Non-Bank CBPS issuers have already applied more optimal ML and TF prevention measures for retail products than for cash products.

Figure 2.4.3.
Risk by Product



According to the heat map of risk presented above, the product considered high risk in terms of ML and TF in the Non-Bank CBPS sector was retail products, while cash was a low-risk product.

4. **ML and TF Risk by Delivery Channel**

ML and TF risks were assessed based on delivery channel in order to explore which delivery channels were most at risk to cases of ML and TF in the Non-Bank CBPS sector. As the object of the risk assessment, the delivery channels were categorised into three groups; Online Merchants, Offline Merchants and ATM (Cash Withdrawals). Risk was assessed as a function of threat, vulnerability and consequence of each respective delivery channel, with the three aspects measured based on predetermined risk factors.

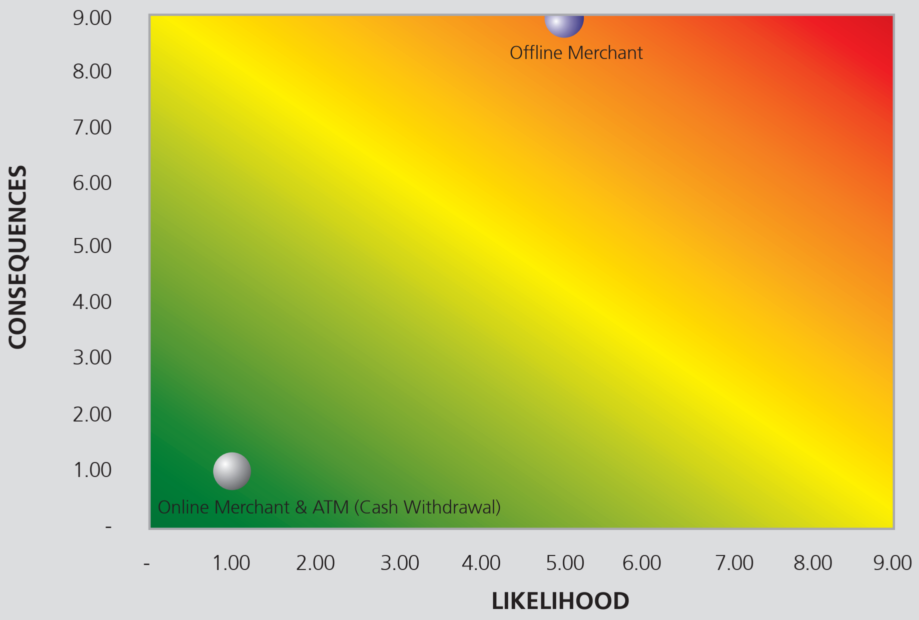
The level of risk was calculated as a function of multiplying the likelihood by the consequences for each respective delivery channel, where the likelihood is the sum of the threat and vulnerability. The following heat map illustrates ML and TF risks in the Non-Bank CBPS sector by delivery channel expressed as a function of threat, vulnerability and consequence (Figure 2.4.4):

According to the heat map of risk presented below, the delivery channel considered high risk in terms of ML and TF incidences in the Non-Bank CBPS sector was Offline Merchants, with the other delivery channels, namely ATM (Cash Withdrawals) and Online Merchants deemed low risk.

Offline Merchants received the highest threat and consequence scores amongst the three delivery channels, accompanied by a medium vulnerability score. The position of Offline Merchants on the x-axis of the heat map demonstrated a higher likelihood than the other delivery channels. Meanwhile, the position on the y-axis of the heat map showed that the consequences of ML and TF in the Non-Bank CBPS sector through Offline Merchants was highest compared with the other delivery channels.

ATM (Cash Withdrawals) and Online Merchants were medium-risk delivery channels in terms of ML and TF incidences in the Non-Bank CBPS sector. In

Figure 2.4.4.
Risk by Delivery Channel



terms of threat and consequence, ATM (Cash Withdrawals) and Online Merchants received low scores. This was explained by the low number of total customers and transaction value using the ATM (Cash Withdrawal) and Online Merchant delivery channels compared with Offline Merchants. Concerning the vulnerability level, however, ATM (Cash Withdrawals) received a high score and Online Merchants a low score. Non-Bank CBPS issuers already apply more stringent treatment of the Online Merchant delivery channels compared with ATM (Cash Withdrawals) and Offline Merchants.

3 RISK MITIGATION

A. Risk Mitigation: Institutional Aspects

1. Non-Bank CBPS issuers operating in Indonesia are required to hold a licence from Bank Indonesia.
2. The management and owners of Non-Bank CBPS issuers are required to meet certain requirements as stipulated by Bank Indonesia as follows:
   a. not registered on the National Blacklist (DHN)[30];
   b. not convicted of certain crimes within the past two years;
   c. fulfilling tax obligations;
   d. free from non-performing loans (NPL);
   e. not declared bankrupt in the 2 years prior to application;
3. Paid-up capital for Non-Bank CBPS issuers must not originate from and/or be used for money laundering purposes.
4. Non-Bank CBPS issuers are required to submit regular and special reports to INTRAC;
5. Non-Bank CBPS issuers are not permitted to issue debit cards or ATM cards.

B. Risk Mitigation: Operational Aspects

1. In practice, cash withdrawal facilities through a credit card are subject to higher interest rates than retail facilities and withdrawal fees.
2. Cash withdrawn using a credit card is limited to 40-60% of the credit limit on the credit card.
3. Cash may only be withdrawn using a credit card from an Automated Teller Machine (ATM) using a Personal Identification Number (PIN). In this case, there are two security elements, namely a CCTV camera fitted to the machine or in the room and a PIN that is known only by the Cardholder.
4. In terms of online e-commerce transactions paid for with a credit card, authentication is achieved using statistical and dynamic data known only by the cardholder. Payment transaction security is provided by two parties, namely the credit card issuer and the e-commerce platform. Transaction security for goods purchased is the responsibility of the e-commerce platform.
5. Credit card facilities are restricted based on customer income. Customers with a monthly income of less than Rp3 million are not eligible for credit card facilities. Customers with a monthly income of Rp3 million - Rp10 million are eligible for a maximum of two credit card issuers. Meanwhile, customers with a monthly income exceeding Rp10 million may simultaneously hold more credit cards.
6. Credit card facilities may be offered to a prospective customer holding a credit card issued by a different bank as a source of customer profile information, including employment details, address, salary slip, income and tax file number.
7. All Non-Bank CBPS Issuers are connected in the AKKI system, which monitors customer and transaction profiles. Therefore, customer profile history can also be monitored.

[30] In accordance with Bank Indonesia Regulation (PBI) No. 18/43/PBI/2016 as an amendment to Bank Indonesia Regulation (PBI) No. 8/29/PBI/2006 concerning the National Blacklist, the National Blacklist contains information regarding all parties withdrawing bad cheques.

8. A text message (SMS) or email notification is sent to the cardholder after every retail transaction and cash withdrawal exceeding a certain threshold.
9. Non-Bank CBPS Issuers are required to maintain a Fraud Detection System (FDS) that can identify and red flag fraudulent and unauthorised transactions.
10. Non-Bank CBPS Issuers are required to identify and verify service users, including legal arrangements, parties acting on behalf of a service user and/or beneficial owners.
11. Non-Bank CBPS Issuers are required to administrate, update and check the List of Suspected Terrorist Organisations and Individuals (DTTOT) and the list of financing of proliferation of weapons of mass destruction against customer information.
12. Enhanced Due Diligence (EDD) is mandatory for high-risk end users.
13. Non-Bank CBPS Issuers are required to implement risk management.
14. Non-Bank CBPS Issuers are required to administrate and exchange information relating to the Credit Card Blacklist.

C. Risk Mitigation: Oversight

1. Bank Indonesia implements on-site and off-site risk-based supervision of AML/CFT application by Non-Bank CBPS Issuers.
2. Bank Indonesia implements thematic supervision of Non-Bank CBPS Issuers.
3. Bank Indonesia may appoint a third party to inspect Non-Bank CBPS Issuers on behalf of Bank Indonesia.
4. For oversight by Bank Indonesia, Non-Bank CBPS Issuers are required to identify, administrate and update data on beneficial owners, while ensuring the availability of such data to Bank Indonesia for supervision purposes.
5. Bank Indonesia crack down cash swipe practices in conjunction with the National Police of the Republic of Indonesia.

4 CONCLUSION

The results of the statistical data analysis to measure the level of ML and TF risk in the Non-Bank CBPS sector based on location, customer profile, product and delivery channel were as follows (Table 2.4.1):

1. **Jakarta** was identified as a **high-risk** region in terms of ML and TF activity in the Non-Bank CBPS sector, followed by Banten and **West Java** (**medium risk**). All other provinces in Indonesia were categorised as **low risk**.
2. In terms of customer profile, **PEPs** and **Private Sector Employees** were considered **high risk** in terms of ML and TF activity in the Non-Bank CBPS sector. All other customer profiles were identified as **low risk**.
3. **Retail** was the product feature identified as **high risk** in terms of ML and TF activity in the Non-Bank CBPS sector. In contrast, cash withdrawals were considered **low risk**.
4. **Offline merchants** were identified as a high-risk delivery channel in terms of ML and TF activity in the Non-Bank CBPS sector. ATM (cash withdrawals) and online merchants were considered low risk.

Table 2.4.1.
SRA Results for Non-Bank CBPS Issuers

SRA Results for Non-Bank CBPS Issuers

Risk	Location	Customer	Product	Delivery Channel
High	Jakarta	PEP and Private Sector Employee	Retail	Offline merchant
Medium	Banten, West Java	-	-	-
Low	Others	Entrepreneur; Bank Employee; Housewife; Professional; Board Member of Foundation, Corporation	Cash Withdrawal	ATM (Cash Withdrawal), Online Merchant

PART 3

BANK INDONESIA ACCOMPLISHMENTS

The prevention and eradication of money laundering and terrorism financing in Indonesia is not a simple undertaking. The relevant government ministries and institutions in Indonesia have implemented a number of strategic policies, detailed as follows, along with some of Bank Indonesia's accomplishments:

1. Bank Indonesia has introduced various mitigation efforts through promulgation of the following regulations concerning payment system service providers and KUPVA BB:
   a. Bank Indonesia Regulation (PBI) No.14/23/PBI/2012 concerning Fund Transfers;
   b. Bank Indonesia Regulation (PBI) No.14/2/PBI/2012, as an amendment to Bank Indonesia Regulation (PBI) No. 11/11/PBI/2009 concerning Card-Based Payment Instruments;
   c. Bank Indonesia Regulation (PBI) No.18/20/PBI/2016 concerning the Operating Activities of Non-Bank Money Changers (PBI KUPVA BB).
   d. Bank Indonesia Regulation (PBI) No.18/9/PBI/2016 concerning Payment System and Rupiah Currency Management Regulation and Supervision;
   e. Bank Indonesia Regulation (PBI) No.18/40/PBI/2016 concerning Payment Transaction Processing;
   f. Bank Indonesia Regulation (PBI) No.19/10/PBI/2017 concerning Anti-Money Laundering and Countering Terrorism Financing (AML/CFT) for Payment System Service Providers and KUPVA BB.
   g. Bank Indonesia Regulation (PBI) No.19/12/PBI/2017 concerning Financial Technology.
   h. Bank Indonesia Regulation (PBI) No.20/2/PBI/2018, as an amendment to Bank Indonesia Regulation (PBI) No.19/7/PBI/2017 concerning Carrying Foreign Banknotes into and out of the Customs Territory of the Republic of Indonesia.
   i. Bank Indonesia Regulation (PBI) No.20/6/PBI/2018 concerning Electronic Money.

2. Bank Indonesia has also published counter-terrorism funding guidelines for payment system service providers and money changers as follows:
   a. Guidelines for Risk-Based AML/CFT Implementation by Supervisors and KUPVA BB and MVTS;
   b. Risk-Based Tools for Supervisors and KUPVA BB and MVTS;
   c. (Updated) Blocking Guidelines for Blacklisted Terrorists and Proliferation of WMD;
   d. Guidelines for the handling of unauthorised KUPVA BB;
   e. Supervision Framework;
   f. Supervision Guidelines for Payment System Service Providers;
   g. Sanction Monitoring Guidelines, including the Monitoring System; and
   h. Circular No. 20/271/DKSP/SRT/B, dated 24th May 2018, announcing Restrictions on Recirculating SGD10,000 Banknotes.

3. Bank Indonesia has also achieved the following accomplishments:
   a. In 2019, Bank Indonesia established the AML/CFT Principles Fulfilment Division. In addition, Bank Indonesia established an interdepartmental

AML/CFT Task Force through a Bank Indonesia Gubernatorial Decree.

b. Bank Indonesia has expanded Memorandums of Understanding (MoU) with Bangko Sentral ng Pilipinas and Bank of Thailand in order to cooperate in terms of AML/CFT implementation.

c. Bank Indonesia has implemented E-Licensing for payment system service providers, KUPVA BB, MVTS and carrying foreign banknotes since 2018.

d. Bank Indonesia has innovated the QR Code into the logos of licensed KUPVA BB and MVTS in order to better distinguish between licensed and unlicensed business entities.

e. Bank Indonesia has restricted the business process of carrying foreign banknotes as an export-import activity into and out of the customs territory of the Republic of Indonesia to authorised business entities up to a value of Rp1 billion. The regulation aims to prevent money laundering, collect statistical data on the process of carrying foreign banknotes and control the circulation of counterfeit banknotes, while strengthening the cash information system.

f. Bank Indonesia is cooperating with the Directorate General of Customs, Ministry of Finance, concerning the carrying of foreign banknotes through three integrated systems, namely Bank Indonesia e-Licensing, Indonesia National Single Window (INSW) as well as the Customs and Excise Information System and Automation (CESA). As of May 2019, a total of 20 business entities had been licensed nationally (8 banks and 12 Non-Bank Money Changers). Based on supervision data, Licensed Entities operating in Jakarta were approved to import foreign banknotes in the fourth quarter of 2018 totalling Rp20 trillion, with a realisation of 66% or Rp13 trillion, and export foreign banknotes totalling Rp16 trillion, with a realisation of 46% or Rp7 trillion.

g. Risk-Based Approach (RBA) to assessing risk profile, supervision and inspections by Bank Indonesia and industry implementation.

h. Joint audit in conjunction with INTRAC and relevant government ministries/institutions concerning KUPVA BB and MVTS.

i. Bank Indonesia is cracking down unauthorised KUPVA BB and illegal MVTS in coordination with the National Police and relevant government ministries/institutions.

j. Bank Indonesia is authorised to impose sanctions (administrative and license revocation) on non-compliant non-bank payment system service providers and KUVA BB.

k. In 2017, the Bank Indonesia Representative Office in Bali closed down Bitcoin ATMs in conjunction with the local police department.

l. Bank Indonesia is providing programmed capacity building to BI supervisors throughout Indonesia as well as personnel from non-bank payment system service providers and KUPVA BB through coordination meetings, workshops and coaching clinics.

m. Bank Indonesia is providing information to fund transfer and money exchange experts regrading criminal cases handled by the police, public prosecutor and judiciary.

n. Bank Indonesia has compiled and implemented the AML/CFT action plan for 2017-2019, with a 100% completion record. The national AML/CFT strategy consists of preparing and implementing RBA, BOG regulations concerning the payment system and rupiah currency management policy framework as well as other regulatory and supervisory provisions; and

o. Restrictions on processing payment transactions using virtual currencies by all payment system operators and FinTech companies in Indonesia.

SECTORAL RISK ASSESSMENT ON MONEY LAUNDERING AND TERRORISM FINANCING: NON-BANK PAYMENT SYSTEM SERVICE PROVIDERS AND MONEY CHANGERS (2019)

ADVISOR
Sugeng - Erwin Rijanto - Filianingsih Hendarta - Pungky P. Wibowo

COORDINATOR AND EDITOR
Ricky Satria - Elyana K. Widyasari - Ronggo Gundala Yudha

DRAFTING TEAM
Garda T. Paripurna - Ginanjar - Dwiyani Sri H.W - Arvi Trianna - Aldo Ersan Mangasi - Gandang D. H. Sugiharto - Muhammad Andrianto E.B.S - Rama Rahadian

OTHER DEPARTMENT CONTRIBUTOR
Financial System Surveillance Department
Regional Department
Bank Indonesia Regional Office

OTHER INSTITUTION CONTRIBUTOR
Indonesian Financial Transaction Reports and Analysis Centre
I Nyoman Sastrawan - Patrick Irawan - Mardiansyah - Ferti Srikandi - Nelmy Pulungan

PRODUCTION TEAM
Feronika Sipayung - Ihsan Karima - Yessy C. Utami

THE PDF FORMAT IS AVAILABLE AT:
http://www.bi.go.id

FOR INQUIRIES, COMMENT AND FEEDBACK PLEASE CONTACT:
Bank Indonesia
Payment System Policy Department
Jl. MH Thamrin No. 2, Jakarta, Indonesia
Email : DKSP-APUPPT@bi.go.id
Phone : 131 (local), 1500131 (international)

BANK INDONESIA
INDONESIAN FINANCIAL TRANSACTION REPORTS AND ANALYSIS CENTRE
2019