BANK INDONESIA

GUIDELINES FOR THE IMPLEMENTATION OF ANTI-MONEY LAUNDERING AND COUNTERING FINANCING OF TERRORISM FOR NON-BANK CARD-BASED PAYMENT INSTRUMENT ISSUERS, ELECTRONIC MONEY ISSUERS AND ELECTRONIC WALLET PROVIDERS

Department of Financial System Surveillance

2019

TABLE OF CONTENTS

ATTACHMENT

CHAPTER I. INTRODUCTION

A. Background

The development of technological innovation boosting the development of financial products and services becomes more advanced and complex, and advances in information technology negating national borders have made organized crime more easily performed across borders (transnational crime), thereby increasing the risks of money laundering and financing of terrorism (ML/FT) encountered by all countries in the world. Money Laundering and Financing of Terrorism are extraordinary crimes that can threaten economic stability and financial system integrity and endanger the pillars of the life of society, nation and state.

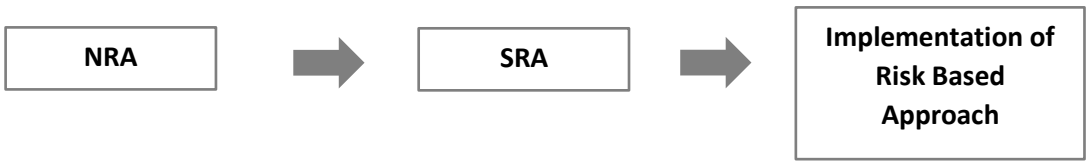
Observing these developments, Financial Service Providers (FSPs) which are under the authority of Bank Indonesia, including Card-Based Payment Instrument (CBPI) Issuers, Electronic Money (EM) Issuers, and Electronic Wallet (EW) Providers in this case classified as Non-Bank Institutions (NBIs), need to improve the implementation quality of risk-based Anti-Money Laundering and Countering the Financing of Terrorism (AML and CFT). Referring to Bank Indonesia Regulation No.19/10/PBI/2017 concerning the Implementation of Anti-Money Laundering and Countering the Financing of Terrorism for Non-Bank Payment System Service Providers (PJSP) and Non-Bank Money Exchange Business Providers and referring to the recommendations and guidelines provided by the international Financial Action Task Force on Money Laundering (FATF), it is expected to be part of the efforts of FSPs and Non-Bank Money Exchange Business in preventing their institutions from being used as a means of ML/FT.

Recommendation No.1 of the FATF confirms that the Provider is required to identify, assess, and understand ML/FT risks related to customers, countries/geographical areas/jurisdictions, products, services, transactions or delivery channels.

Along with efforts to prevent and eradicate ML/FT crimes in Indonesia and fulfill Indonesia's commitment to the implementation of Recommendation No.1 of the FATF, INTRAC/PPATK together with other AML and CFT stakeholders conducted an Indonesian risk assessment of the ML/FT crimes in the form of a National Risk Assessment (NRA) in 2015 and was updated in 2019. Following up on the results of the NRA, Bank Indonesia has updated the Sectoral Risk Assessment (SRA), especially in the Non-Bank Fund Transfer and Money Exchange businesses , which was completed in May 2017.

Furthermore, to ensure that the risks posed by criminal acts that occur remain the most recent, the INTRAC together with other relevant AML and CFT stakeholders has carried out an update of Indonesia's risk assessment of ML/FT crimes in the form of Updated 2015 NRA. Following up on the update of the NRA, Bank Indonesia has updated the Sectoral Risk Assessment (SRA) level in a number of supervised sectors, including preparing SRAs for CBPI Issuers, EM Issuers and/or EW Providers.

The NRA and SRA are used as a reference in the implementation of Risk-Based Approach (RBA) by the Supervisor and Provider. The updating of the NRA and SRA will be conducted periodically and will be disseminated by the competent Supervisory and Regulatory Authority (LPP).



B. Objectives of the Guidelines for the Implementation of Risk-Based AML and CFT Program

The objectives of the Guidelines for the Implementation of Risk-Based AML and CFT Program for CBPI Issuers, EM Issuers and EW Providers are:

1. As guidelines for identifying, understanding and carrying out ML/TF risk mitigation measures and financing of weapons of mass destruction proliferation; and
2. As technical guidelines in the business activities of CBPI Issuers, EM Issuers and EW Providers.

In accordance with Article 7 paragraph 5 PBI No.19/10/PBI/2017 concerning the Implementation of Anti-Money Laundering and Combating the Financing of Terrorism for Non-Bank Payment System Service Providers and Non-Bank Money Exchange Business Providers (PBI AML and CFT), the implementation of risk management are based based on the characteristics, scale and complexity of the business activities of the Providers, as well as relevant risk exposures that are previously **consulted or determined by Bank Indonesia supervisors**.

CHAPTER II. IMPLEMENTATION OF RISK-BASED AML AND CFT PROGRAM

The implementation of risk-based AML and CFT Program by CBPI Issuers, EM Issuers and EW providers generally refers to the risk management process and specifically refers to the FATF guidelines related to Risk Based Approach. The process starts from monitoring, on-site examination and evaluation. Monitoring covering five important aspects of a business operation, i) the active role of the board of directors and commissioners, ii) written policies and procedures as internal guidelines, iii) the risk management process itself, iv) human resource management that ensures the quality of implementation and v) internal control as a control process.

A. Duties and Responsibilities of the Board of Directors and Active Supervision of the Board of Commissioners

In implementing AML and CFT Program, the Boards of Directors of CBPI Issuers, EM Issuers, and EW providers are responsible for:

1. Establishing written policies and procedures for the implementation of AML and CFT Program based on the approval of the Board of Commissioners.

   Issuers/Providers to complete written policies and procedures with written authorization from the Board of Directors. As for the scope of written policies and procedures, it will be explained in more detail in part B.

2. Ensuring that the implementation of the AML and CFT Program is carried out in accordance with established written policies and procedures.

   The Board of Directors needs to ensure that the implementation of established written policies and procedures is implemented effectively. One way to ensure the effectiveness of the implementation of the AML and CFT Program is to implement a reporting mechanism related to AML and CFT from the work unit/Board of Directors/Executive Officers responsible for implementing the AML & CFT Program to the Board of Directors. Based on the report submitted, the Board of Directors can assess whether the implementation of the AML and CFT Program is in accordance with written policies and procedures.

3. Adjusting written policies and procedures regarding AML and CFT Program in line with changes and development of products, services, technology, ML/FT mode and applicable provisions related to AML and CFT.

   The provider needs to ensure that written policies and procedures are in accordance with the applicable provisions and current business conditions. Adjustments to written policies and

procedures are particularly necessary when there is a change in business activities and business scale, for example, when the Provider markets new products or services. CBPI Issuers, EM Issuers, and EW providers also need to make adjustments to written policies and procedures whenever there is a change in provisions by the competent authority. For this reason, evaluations of written policies and procedures need to be conducted periodically. The Provider must submit an adjustment to written policies and procedures no later than 10 (ten) working days after the adjustment is made to Bank Indonesia.

4. Conducting an analysis of Suspicious Transaction Report (STR), Cash Transaction Report (CTR) for cash transactions above Rp500 million, and International Fund Transfer Instruction (IFTI) as well as reporting these reports to INTRAC.

   The Board of Directors is responsible for ensuring that the reports have been submitted in an orderly manner to INTRAC in accordance with the provisions. Information regarding the submission of these reports should also be reported in reports from work units/Executive Officers responsible for implementing the AML and CFT Program to the Board of Directors.

5. Ensuring the implementation of blocking immediately (freeze without delay) and submitting reports of transaction freezes, blocking of transactions and/or rejection of transactions against the List of Terrorist Suspects and Terrorist Organizations (DTTOT) and the list of funds for the proliferation of weapons of mass destruction.

   Based on DTTOT information and a list of funding for the proliferation of weapons of mass destruction received, the Provider is required to carry out a blocking immediately (freeze without delay) of the assets listed on:

   a. Suspected terrorists and/or terrorist organizations listed in DTTOT, as issued by the Head of the Indonesian National Police with reference to United Nations Security Council Resolutions (UNSCRs).
   b. Financing for the proliferation of weapons of mass destruction.

   Subsequently, the Provider shall submit reports on transaction freezes, transaction blocking, and/or transaction refusal of assets listed in:

   a. DTTOT; to the Head of Special Detachment (*Densus*) 88 AT with a copy to Bank Indonesia,
   b. List of financing for the proliferation of weapons of mass destruction; to the Head of INTRAC with a copy to Bank Indonesia.

6. Ensuring that all employees have obtained knowledge and/or training regarding the implementation of the AML and CFT Program.

The effective implementation of AML and CFT Program needs to be supported by a good understanding of the urgency of the AML and CFT Program by Employees. For this reason, the Board of Directors is responsible for ensuring that the provision of knowledge and/or training regarding AML and CFT to Employees is conducted regularly and continuously.

7. Updating Service User profiles and Service User transaction profiles.

   The Provider must have mechanisms and tools for recording the profile and transactions of service users. The Provider may use at least a data processing implementation (spreadsheet) as a tool in maintaining and updating the profiles of Service Users and their transactions. If it is based on monitoring unusual transactions or transactions that do not match the User Profile, the Provider verifies the User Profile. The mechanism for monitoring and updating the profiles of Service Users and their transactions should be included in the scope of written policies and procedures.

The Board of Commissioners conducts active supervision over the implementation of the AML and CFT Program, including:

1. Granting approval for written policies and procedures for the implementation of the AML and CFT Program.

   CBPI Issuers, EM Issuers and EW Providers must complete written policies and procedures for the implementation of the AML and CFT Program with the approval sheet from the Board of Commissioners.

2. Supervision of the implementation of the Board of Directors' responsibility for the implementation of the AML and CFT Program.

   The Board of Commissioners can ensure that the Board of Directors has performed the responsibility of implementing the AML and CFT program, among others through minutes of meetings, if the report is submitted at the meeting, or a written report from the Board of Directors to the Board of Commissioners.

B. Written Policies and Procedures

In order for the AML and CFT Program to be applied effectively by the Provider, written policies and procedures are determined by the Directors based on the approval of the Board of Commissioners as references. The scope of written policies and procedures includes the following:

1. Customer Due Diligence (CDD)

To Service Users who have a business relationship with CBPI Issuers, EM Issuers and EW Providers, it is carried out by requiring the submission of data and information which at least includes:

Individual Customer	Corporate Customer	Other Customers
Full name including an alias, if any	Name of corporation	Name
Identification document number	Form of legal or business entity	License number from the competent authority (if any)
Address of residence in accordance with identity documents and other residential addresses, if any	Place and date of incorporation	Office address
Place and date of birth	Business license number	Form of engagement
Citizenship	Domicile address	Data and information on the identity of individuals authorized to act for and on behalf of other commitments
Phone Number	Phone number	-
Work	Type of business field or activity	-
Gender	Names of Management and Shareholders	-
Signature or biometric data	Data and information on the identity of individuals authorized to act for and on behalf of the Corporation	-

To identify the Service Users above, the Issuer/Provider must ask the Service User to submit an identity document in the form of (choose one):

Individual Customer	Corporate Customer	Other Customers
ID Card	Memorandum of Association and/or Articles of Association	Proof of registration with the competent authority
Driving License	Business license or other permits from the competent authority	Memorandum of Association and/or Articles of Association
Passport	TIN for those who are required to TIN according to the Taxation Law	Personal identification documents (in accordance with PBI AML and CFT)
Other documents issued by government agencies	Identity documents of individuals authorized to act for and on behalf of the Corporation	

If it is based on an analysis taking into account factors such as occupation/profession, citizenship, behavior, transaction pattern, etc., the Issuer/Provider concludes that a Service User is categorized as a high risk, then the Issuer/Provider is required to:

a. obtain additional information about the Service User profile;
b. update identity data more routinely;
c. obtain additional information regarding the intent and objectives of the business relationship or transaction;
d. obtain additional information about sources of funds and sources of wealth; or
e. conduct more rigorous monitoring of business relationships or transactions including determining transaction criteria that need to be further analyzed.

If the Issuer/Provider suspects that the Service User is conducting transactions related to ML/FT which if the performance of CDD can cause the Service User to realize that the Provider has suspected the Service User, then the Issuer/Provider is able to cease **the CDD process, complete the transaction and must report the transaction as a ST to INTRAC**.

2. Enhanced Due Diligence (EDD)

EDD must be performed on high-risk service users, namely:

a. High-risk BOs/service users (PEPs or their families or related parties, high-risk business fields, appointing third parties to conduct transactions, listed in DTTOT and/or financing of the proliferation of weapons of mass destruction);
b. High-risk countries (on the NRA/SRA list, as well as FATF, World Bank, OECD, and other credible international institutions);
c. High-risk products/services (priority customers, anonymous transactions, etc.);
d. Delivery channels (large amounts of transactions, distribution channels in NRA/SRA);

In conducting EDD, the Provider requests additional information in the form of funding sources, and the purpose of the transaction.

3. Rejection of transaction

The Provider rejects/cancels the customer's transaction, if:

a. Customer does not provide identity data.
b. Customer uses a fictitious/anonymous name.
c. The Provider doubts the validity of the customer's identity.

The authority of the Issuer/Provider to refuse, cancel, and/or close business relations with Service Users, must be stated in the account opening agreement (terms and conditions) and notified to the User.

4. Anti tipping-off.

Issuers/Providers are prohibited from notifying Service Users or any other parties, directly or indirectly, in any way regarding Suspicious Transaction Reports that are being prepared or submitted to INTRAC.

5. Management of data, information and document

Issuers/Providers are required to keep documents related to customer data for at least 5 (five) years and documents related to customer transactions for 10 (ten) years. Documents related to customer data include:

a. Service User ID including supporting documents.
b. Proof of verification of User Data;
c. Results of monitoring and analysis that have been carried out;
d. Correspondence with Service Users; and
e. Documents related to reporting Suspicious Transactions.
f. Related to Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction, Providers must administer copies of the Minutes submitted, lists of

suspected terrorists and terrorist organizations, and lists of funds for proliferation of weapons of mass destruction, and use the list of results of the administration in checking the suitability of customer data.

6. Reporting

Providers must submit reports on the implementation of AML and CFT on an annual basis to Bank Indonesia no later than January of the following year, and other reports stipulated in the provisions.

C. Risk Management Process

In the implementation of risk management, Providers must take 5 (five) steps, namely:

1. Risk identification

In identifying risks, Providers must consider the risks caused by service users, countries/regions, products or services, and transaction networks. In detail, it can be described as follows:

a. Service user risk

Assessment of the Risk of Service Users is carried out by comparing the number of Service Users who have high-risk professions referring to the SRA and Service Users who are the citizens of high-risk countries referring to the NRA with the total Service Users. The data that must be prepared by the Provider is in the form of:

Parameter	CBPI Issuer	EW Issuer and/or EW Provider
The composition of the service user profession	• Total service users per profession • Number of service users for private employees, entrepreneurs, professionals, bank employees, and other professions	
The composition of citizenship of service users	• Total service users per country • The number of users of Indonesian citizens, North Korea, Iran, Syria, Tunisia, Yemen, the Bahamas, Botswana, Cambodia, Ethiopia, Ghana, Pakistan, Serbia, Sri Lanka, Trinidad Tobago and other foreigners.	

b. Country or geographic area risk

The location where Providers operate has the potential to have a high risk of money laundering and/or financing of terrorism activities. Areas that are known to have high crime rates and/or are located in border areas between countries have the potential to

have a higher ML/FT risk. The country and geographical area are also one of the parameters in the SRA, so the results of the SRA are the main reference in determining the parameters for assessing the geographical risk level of a Provider as follows:

Parameter	CBPI Issuer	EW Issuer and/or EW Provider
Location of customer's domicile	The number of customers domiciled in DKI Jakarta, Banten, West Java, and others.	Number of business locations in DKI Jakarta, Banten, West Java, North Sumatra, Bengkulu, Bali, Riau Islands, and others.

c. Product/service risk

The products and/or services offered by Providers have the potential to be utilized in money laundering or financing of terrorism activities. Product and/or service risk assessment is carried out using the mechanism parameters, value, volume, and type of transaction. The data that must be prepared by the Provider is in the form of:

Parameter	CBPI Issuer
Payment method	• Nominal cash payment outside the bank or issuer • Nominal transfer payments through the bank
Cash advance limit	• Percentage of cash advance to the limit given to Users.
Number of cards	• Number of credit cards is based on the limit of credit cards issued
Number of overpayment customers	• Number of debit customers (having a debit/debt balances) • Number of credit customers (having credit/credit balances) that overpayment based on card limits
Nominal Transaction	• Nominal domestic transactions per category (shopping or cash advance). • Nominal foreign transactions per category (shopping or cash advance).

Parameter	EW Issuer and/or EW Provider
Nominal top Up	• Nominal cash top up • Nominal non-cash top up
Nominal Transaction	• Nominal transactions are based on top up, transfer to account categories, transfers between EM, spending, cash withdrawals and redeem.
Volume or Frequency of Transactions	• Volume or frequency of transactions based on top up, transfers to account, transfers between EU, spending, cash withdrawals, and redeem.
Cross-Border Transaction Feature	• The presence of cross-border transaction features
EW nominal transaction	• EW nominal transactions for credit cards, debit cards, other EM issuers, EM own products, virtual accounts, and others.
The volume or frequency of EW transactions	• EW volume or frequency for credit cards, debit cards, other EM issuers, own EM products, virtual accounts, and others.

d. Delivery Channel

A transaction network is a medium for carrying out transactions of a product or service. High risk is inherent in the delivery channel that allows transactions to occur without going through an adequate CDD process, for example transactions that are entirely in an offline merchant. This risk may also arise from the number of cash out service points, as well as the number of principals at CBPI. The more the number of cash out service points and the number of principals, will increase the level of risk because there are risks of increasing non-compliance with AML and CFT requirements, and increasing the need for Provider control over service points and/or partners. The data that must be prepared by the Provider is in the form of:

Parameter	CBPI Issuer
Distribution or marketing methods	• Number of issuers and 3rd parties brokering CBPI, EM and/or EW marketing
Nominal Transaction	• Number of offline merchants • Number of online merchants
Number of principals	• Name of principal

Parameter	EW Issuer and/or EW Provider
Number of merchants	• Number of offline merchants • Number of online merchants
Number of cash out channels	• Number of cash out channels owned by the Issuer • Number of cash out channels outside the Issuer
Nominal and frequency of transactions at merchants	• Nominal and transaction frequency at offline merchants • Nominal and transaction frequency on the number of online merchants

e. Politically Exposed Person (PEP)

Politically Exposed Person or PEP include:

(1) Foreign PEP is a person who is given the authority to perform prominent functions by another country;

(2) Domestic PEP is a person who is given the authority to perform prominent functions by the country; and

(3) People who are given the authority to perform prominent functions by international organizations.

The presence of PEP will increase the level of risk because there is a risk of using Issuer/Provider's products by PEP to carry out ML/FT. The data that must be prepared by the Provider is in the form of:

Parameter	CBPI Issuer	EW Issuer and/or EW Provider
PEP	Number of PEP	

After collecting data, Providers must calculate the inherent risk value they have by entering data in the RBA tool prepared by Bank Indonesia (**Appendix 1** of the Risk Assessment Form). Risk values can be divided into 3, namely Low, Medium and High.

Low	Medium	High
Description: Issuers/Providers are exposed to ML/FT risks but are classified as low. Action: Issuers/Providers operate the PBI AML & CFT and adequate monitoring.	Description: Issuers/Providers are exposed to medium-scale ML/FT risks. Action: Issuers/Providers carry out monitoring efforts and endeavors to prevent increased risks. For example: socialization to regular employees regarding guidelines for implementing AML & CFT.	Description: Issuers/Providers are exposed to high-scale ML/FT risks. Action: Issuers/Providers make special and maximum efforts to implement tighter risk mitigation in order to reduce these risks. Example: applying a transaction limit on a cash out transaction.

2. Assessment

Furthermore, Issuers/Providers self-assess the implementation of the AML & CFT Program to assess compliance with applicable regulations by answering the questionnaire on the Self-Assessment form provided by BI (**Appendix 2** of the Self-Assessment Form).

The assessment is based on the Providers' compliance with: (a) Active supervision by the Board of Directors and the Board of Commissioners; (b) Written Policies and Procedures; (c) Risk Management; (d) Human Resources; (e) Internal Control.

The evaluation criteria are as follows:

FINAL SCORE	GRADE
1 - 1.8	*Strong*
>1.8 - 2.6	*Satisfactory*
>2.6 - 3.4	*Fair*
>3.4 - 4.2	*Marginal*
>4.2 - 5	*Unsatisfactory*

3. Control

The control phase is the stage to make improvements to the results of self-assessment. Issuers/Providers must cover the deficiencies in the five aspects of compliance above. For example, if Issuers/Providers have not provided AML & CFT training to employees, the Issuers/Providers must immediately provide training to employees. If the Board of Directors has not given approval to the SOP for AML & CFT implementation, the board of directors must immediately determine the latest SOP and signed off with the commissioners.

4. Risk Mitigation

a. Planning and implementing risk mitigation

At the risk identification stage, Issuers/Providers can assess the risks inherent in their business. Therefore, Providers must determine and implement steps to deal with the risks referred to, for example:

- Issuers/Providers do not provide cash out limits on offline merchants. Therefore, Issuers/Providers must impose a maximum transaction limit of Rp10 million/person/day.
- To ensure that all employees understand and can apply SOP correctly, Providers conduct refreshment program to employees every 3 months. The AML & CFT work units at the head office carry out regular monitoring of the correctness of user data input by employees at all service points.
- Monitoring and evaluating the implementation of the risk-based approach.
  Issuers/Providers must monitor the implementation of the risk-based approach in the implementation of the AML and CFT Program of the Issuers/Providers. Monitoring the implementation of risk management is carried out by the work unit responsible for

implementing the AML & CFT program. Furthermore, the results of such monitoring must be reported to the Directors and Commissioners so that they can carry out their duties to oversee the implementation of the AML & CFT program. Issuers/Providers must re-evaluate risk identification, mitigation, procedural policies and internal controls if there is a change in the structure and scale of business activities or the development of new products.

D. HR Management

Human resource management, at least includes:

1. Screening in the context of recruitment (pre-employee screening);
   Issuers/Providers are required to screen prospective employees, including ensuring that prospective employees have never been involved in ML/FT activities and by comparing their identities with DTTOT.
2. Monitoring employee profiles:
   Issuers/Providers must constantly monitor employee profiles including profiling data on employee identity and competencies.
3. Training programs and increasing employee awareness on an ongoing basis.
   There are several methods for increasing AML and CFT knowledge to employees, for example through discussions, workshops, training, self-learning, e-learning and so on. For example, employees can obtain knowledge about AML and CFT through the websites of INTRAC and/or Bank Indonesia. The training program and understanding improvement must be carried out regularly as evidenced by the minutes/work program, documentation in the form of photos, attendance list signed by employees who have participated in training/knowledge sharing.

E. Internal Control

Internal control system, at least includes:

1. Issuers/Providers must have the function responsible for the implementation of AML and CFT. The designated function should be adjusted to the business scale of Issuers/Providers, which can be in the form of a work unit or by appointing directors/executive officers to be responsible for the implementation of the AML and CFT Program. Establishment/appointment of the person in charge of AML & CFT followed by written documents, including the Board of Directors' Decree which designates the names and job descriptions of AML & CFT officers; the name of AML and CFT officers in the AML CFT SOP;

the name of the person in charge, the contact person and the reporting officer to the GRIPS-INTRAC registration.

2. The audit function in Issuers/Providers must have a clear separation of duties and authority between the units that function as internal audits and the business units of the Providers which carry out operational activities.
3. Providers must be periodically audited by an independent party (external party or an independent party within the company) according to the scale of business of the Provider.
4. Reporting

   Issuers/Providers are required to meet routine reporting in accordance with the provisions and according to the specified schedule, both routine and incidental reports requested by the regulator.

   a. Report to BI:
      1) Reports on changes to written policies and procedures on the implementation of AML & CFT shall be submitted no later than 10 days after the changes.
      2) Annual reports on the implementation of AML & CFT are reported no later than January of the following year. BI provides the report format in Appendix 3 (Annual Report on the Implementation of the AML & CFT Program).
      3) Transaction freeze reports, account freezes, and/or rejection of transactions related to DTTOT and a list of financing of the proliferation of weapons of mass destruction shall be submitted no later than 10 days after the said action.
      4) Other reports.
   b. Report to INTRAC:
      1) STR
      2) CTR
      3) IFTI
      4) SIPESAT
      5) Other reports
5. Information and data systems

   Considering the complexity of the RBA process, Issuers/Providers require a special implementation to be able to carry out monitoring especially for providers who have a complex business scale (as shown in the number of cash out service points, type of transaction, service user, number of products, type of currency, large geographical area). To

facilitate the processing of Issuers/Providers' data which currently does not have a special implementation, Bank Indonesia provides a spreadsheet format. Providers must be disciplined to be able to implement it effectively.