BANK INDONESIA

# GUIDELINES FOR THE IMPLEMENTATION OF RISK BASED APU AND PPT ON NON-BANK MONEY VALUE TRANSFER SERVICES AND FOREIGN EXCHANGE BUSINESS ACTIVITY OPERATORS

Guidelines for the Implementation of Risk Based Approach Related to the Implementation of APU & PPT Program in the Non-Bank Money Value Transfer Service and Foreign Exchange Business Activity Operators

**Payment System Policy and Supervision Department**

**2017**

# CHAPTER I. INTRODUCTION

## A. Background

The development of technological innovations has encouraged the development of financial products and services to become more advanced and complex, and the advancement of information technology that eliminates state boundaries has resulted in the facilitation of transnational organized crime, thereby increasing the risk of money laundering and financing terrorism (PU/PT) facing all countries in the world. Money laundering (TPPU) and Criminal Acts of Terrorism Financing (TPPT) is an extraordinary crime that can threaten the stability of the economy and the integrity of the financial system, and can endanger the joints of life in society, nation and state.

In response to these developments, the Financial Services Providers (FDD) which are under the authority of Bank Indonesia, such as Non-Bank Money Value Transfer Services and Foreign Exchange Business Activity Operators shall improve the quality of risk-based Anti-Money Laundering and the prevention of Terrorism Financing (APU and PPT) program. With reference to Bank Indonesia Regulation No.I9/10/PBI/2017 concerning Implementation of Anti-Money Laundering and Prevention of Terrorism Financing for Non-Bank Payment System Service and Foreign Exchange Business Activity Operators as well as referring to the recommendations and guidelines provided by international financial institutions namely the Financial Action Task Force on Money Laundering (FATF), is expected to be one of the efforts of Non-Bank Payment System Service Provider and Foreign Exchange Business Activity Operator in preventing its institution to be used as PLI/PT.

Recommendation No.1 of FATF asserts that the Obligatory Operator identifies, assesses, and understands the risks of PU/PT in relation to customers, countries/geographical areas/jurisdictions, products, services, transactions or distribution channels.

In line with the efforts to prevent and eradicate TPPU and TPPT in Indonesia and to fulfill Indonesia's commitment to the implementation of Recommendation No. 1

FATF, by 2015 PPATK together with APU and other PPT stakeholders have conducted an assessment of Indonesia's risk to TPPU and TPPT in the form of National Risk Assessment (NRA). Following up on the results of the NRA, Bank Indonesia has conducted Sectoral Risk Assessment (SRA) especially in the Non-Bank MVTS and Foreign Exchange Business Activity Operators sector which was completed in May 2017.

The NRA and SRA are used as guidelines in the application of APU and Risk Based Approach (RBA) by the Supervisor and the Operator. The updated NRA and SRA will be conducted periodically and socialized by the Supervisory Board and Regulatory Authority (LPP).

NRA → SRA → Application of Risk Based Approach

B. Objectives of the Implementation of Risk Based APU and PPT Program

The Objectives of Guidelines for Risk-Based APU and PPT Program for MVTS and Money Changers operators are:

1. To serve as guidelines for identifying, understanding and undertaking risk mitigation measures of PU/PT and funding the proliferation of weapons of mass destruction.
2. To serve as a technical guideline in the business activities of Non-Bank MVTS and Foreign Exchange Business Activity Operators.

Pursuant to paragraph 5 article 7 of PBI of APU & PPT No 19/10/PBI/2017 concerning Implementation of Anti Money Laundering and Prevention of Terrorism Financing for Non-Bank Payment System Service Provider and Foreign Exchange Business Activity Operator, the implementation of risk management based on characteristics, scale, and complexity of the Operator's business activities, as well as relevant risk exposure prior to consultation or determination by BI supervisors.

## CHAPTER II. IMPLEMENTATION OF RISK BASED APU & PPT PROGRAM

The application of risk-based APU & PPT programs by Non-Bank Payment System Service Provider and Foreign Exchange Business Activities Operator generally refers to the risk management process and specifically refers to the FATF guidelines related to Risk Based Approach. The process begins with monitoring, assessment and monitoring covering five important parts of a business operation that is the active role of the board of directors and commissioners, the existence of written policies and procedures as internal guidelines, the risk management process itself, the Human Resource management that ensures the quality implementation and internal control as a control process.

A. Duties and Responsibilities of Board of Directors and Active Supervisory of Board of Commissioners

In implementing the APU and PPT program, the Board of Directors of the Operator is responsible for:

1. To stipulate written policies and procedures for the implementation of APU and PPT programs based on the approval of the Board of Commissioners.

   Operator shall complete written policies and procedures with written approval from the Board of Directors. The scope of written policies and procedures will then be explained in detail in section B.

2. To ensure the implementation of APU and PPT programs is implemented in accordance with written policies and procedures established.

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

3. To adjust written policies and procedures regarding APU and PPT programs in line with changes and development of products, services, technology, PU/PT mode and applicable provisions related to APU and PPT.

   Operator needs to ensure that written policies and procedures are in accordance with the terms and conditions of the current business. Adjustment of written policies and procedures is particularly necessary when there are changes to business activities and business scale, for example, when the Operator markets a new product or service. Operators also need to make adjustments to written policies and procedures whenever there is a change of provision by the competent authority. For that evaluation of written policies and procedures need to be done periodically.

   Operator shall submit adjustments to written policies and procedures no later than 10 (ten) working days after the adjustment is made to Bank Indonesia.

4. To submit Suspicious Financial Transactions Report (LTKM), Cash Financial Transactions (LTKT) for cash transactions above Rp500million, Transactions from/to overseas (LTKL) to PPATK.

   The Board of Directors is responsible for ensuring that the reports have been submitted in an orderly manner to the PPATK in accordance with the provisions. Information on the submission of these reports is also reported in the report of the work unit/Directors/Executive Officers responsible for the implementation of the APU & PPT program to the Board of Directors.

5. Ensure the execution of blocking and promptly submitting reports of transaction freezing, transaction blocking and/or rejection of suspected Terrorist Listings and Terrorist Organizations (DTTOT) and list of funding for the proliferation of weapons of mass destruction.

   Based on the DTTOT information and list of funding of the proliferation of weapons of mass destruction received, the Compulsory Operator implements a blocking of assets immediately:

a. Alleged terrorist and/or terrorist organizations listed in DTFOT, as issued by the Chief of Police of the Republic of Indonesia with reference to United Nations Security Council Resolutions (UNSCRs).

b. Funding the proliferation of weapons of mass destruction.

Further, the Operator submits a report on the freezing of the transaction, the transaction blocking, and/or the transaction's denial of the assets listed in:

a. DTTOT; to the Chief of Police with a copy to Bank Indonesia,

b. List of funding of proliferation of weapons of mass destruction to PPATK with carbon copy to Bank Indonesia.

6. To ensure that all employees have obtained knowledge and/or training on APU and PPT program implementation.

   Effective APU and PPT program implementation must be supported by a good understanding of the urgency of APU and PPT programs by the Employees. To that end, the Board of Directors is responsible for ensuring that the provision of knowledge and/or training on APU and PPT to the Employees is conducted periodically and continuously.

7. To update the Service User Profile and Transaction Profile of the Service User.

   Operator must have mechanisms and tools for recording the profiles and transactions of Service Users. Operator may use at least a data-processing application (spreadsheet) as a tool in maintaining and updating the Service User Profile along with its transactions. If on the basis of monitoring found transactions that are not fair or inappropriate profile of Service User, Operator verifies Profiles of Service Users. The monitoring mechanism and updating of User Profile profiles and their transactions should be within the scope of written policies and procedures.

The Board of Commissioners exercises active supervision on the implementation of APU and PPT programs, including:

1. Approval of written policies and procedures for the implementation of APU and PPT programs.

   Operator to complete the written policies and procedures for the implementation of the Anti-Money Laundering and Counter-Terrorism Financing Program with the approval from the Board of Commissioners.

2. Supervision of the implementation of the Board of Directors' responsibilities towards the implementation of APU and PPT programs.

   The Board of Commissioners shall ensure that the Board of Directors has carried out the responsibilities of the APU and PPT Program implementation among others through minutes of meetings, if reports are submitted in meetings or written reports of the Board of Directors to the Board of Commissioners.

B. Written Policy and Procedures

In order for the implementation of APU and PPT programs by the Operator can be effectively implemented, required written policies and procedures established by the Board of Directors based on the approval of the Board of Commissioners as a reference. The scope of written policies and procedures among others is as follows;

1. Customer Due Diligence (CDD)

   With respect to a Service User who makes transactions less than Rp100,000,000.00 (one hundred million rupiah) and does not have a walk-in customer relationship is done by requiring the submission of data and information at least:

| Individual Customer | Corporate Customer | Other Customer |
|---|---|---|
| Full name including alias if any | Name of corporation | Name |
| Identity Document Number | Address and Domicile, if any | Address of domicile |
| Residential address | Identity Data and Information of | Identity Data and |

| | | |
|---|---|---|
| according to identity documents and residential address if any | the Natural Person acting for and on behalf of the Corporation | Information of the Natural Person acting for and on behalf of other engagements |
| Place and Date of Birth | - | - |
| Signature and Biometric Date | - | - |

If based on analysis with consideration on factors such as occupation/profession, citizenship, behavior, transaction pattern, etc. Operator concludes that a Service User is at high risk, so Operator to:

a. obtain additional information about the Service User Profile;

b. regularly updating identity data;

c. obtain additional information regarding the intent and purpose of the business relationship or transaction;

d. obtain additional information on sources of funds and sources of wealth; or

e. conduct more strict monitoring of business relationships or transactions including specifying transaction criteria that need to be analyzed further.

If the Service User or Beneficial Owner is included in the Politically Exposed Person (PEP) category, the Operator shall perform EDD for PEP as will be further described.

For service users outside the criteria as outlined in the first paragraph above, the Operator shall require additional information such as follows:

| Individual Customer | Corporate Customer | Other Customer |
|---|---|---|
| Nationality | Type of corporation | Legal Arrangement |

| | | |
|---|---|---|
| Telephone Number | Place and date of Incorporation | - |
| Occupation | Business Permit Number | - |
| Gender | Line of Business/Activity | - |
| - | Telephone Number | - |
| - | Name of managers | - |
| - | Name of Shareholders | - |

The identification and verification of customer data in fund transfer activities follow the procedures set forth in the provisions.

If a Operator suspects a Service User of a PU/PT-related transaction which, if done by the CDD, may cause the Service User to realize that the Operator has suspected the Service User, the Operator may terminate the CDD process, settle the transaction and Obligate to report the transaction as TKM to PPATK.

Especially for the transfer of funds, the process of identification/verification shall be done by the Initially Sending Operator and the Final Receiving Operator. Information transmitted by the original sender Operator to the successor Operator or the ultimate beneficiary operator is at least as follows:

a. Initially sending Operator (for cross border transactions <Rp10 million, then only the sender's name);

b. unique sender account/reference number;

c. recipient's name;

d. unique recipient's account/reference number.

2. Enhanced Due Diligence (EDD)

EDD must be conducted for high-risk users:

a. High-risk service/RB users (PEP or their families or related parties, high risk business areas, appoint a third party to conduct transactions, are listed in DTTOT and/or funding the proliferation of weapons of mass destruction;

b. High risk countries (in NRA/SRA lists, as well as FATF, World Bank, OECD, and other credible international institutions);

c. High risk products/services (priority customers, anonymous transactions, etc.);

d. Distribution channels (large number of transactions, distribution channels within the NRA/SRA);

e. It is alleged to be unauthorized parties, such as illegal Money Value Transfer Services Operator, unlicensed Foreign Exchange Business Activity, and other Payment System Service Provider;

In performing EDD, the Operator requests additional information in the form of a source of funding, and the purpose of the transaction,

3. Rejection of transaction

Operator refuses/cancels a customer transaction, if

a. The Customer does not provide identity data.

b. Customer uses a fictitious/anonymous name.

c. Operator doubts the identity of the customer.

4. Anti-Tipping-off.

Operator is prohibited from notifying Service Users or any other parties, either directly or indirectly, in any way concerning the Suspicious Financial Transactions report being prepared or submitted to the PPATK.

5. Data, information, and Document Management

The Operator shall keep documents related to the customer's data at least 5 (five) years and documents related to customer transactions during WO (ten) years. Documents related to customer data including:

a. User Identity of Service including supporting documents.

b. Proof of verification of Service User data;

c. Result of monitoring and analysis which have been done;

d. Correspondence with Service Users; and

e. Documents related to Suspicious Financial Transaction reporting.

f. Related to Terrorism Financing and Funding of Weapons of Mass Destruction Proliferation, Operators are required to administer a list of suspected terrorists and terrorist organizations and funding lists of weapons of mass destruction proliferation, and use the list of administrations to check the suitability of customer data.

6. Reporting

The Operator shall submit annual reports on the application of the APU and PPT on the latest by December of the current year, and other reports provided for in the provisions.

C. Risk Management Process

In performing risk management, Operator must perform 5 (five) steps, namely:

1. Risk Identification

In performing risk identification, the Operator should consider the risks caused by the service user, country/region, product or service, and transaction network. In detail, it can be described as follows:

a. Service user risk

Assessment of User Service Risk is done by comparing the number of Service Users who have high risk profession referring to SRA and Users of Service which is a high-risk country which refers from NRA with total Users of Service. The data must be prepared by the Operator in the form of:

| Parameter | Non-Bank MVTS | Non-Bank Money Changers |
|---|---|---|

| | |
|---|---|
| Composition of service user profession | • Total Service User<br>• Number of service users each employed as private employee, entrepreneur, in the form of corporation, housewife, foundation/caretaker of foundation, PEP, other profession |
| Nationality Composition | • Total Service User<br>• Number of service users of Indonesian, North Korea, Iran, Syrian, Myanmar, Afghan, Sudan, Cuban, British Virgin Island, Cayman Island, Nigerian Nationals, and other foreigners. |

b. Country or geographical area risk

Locations where Operators operate have the potential to have a high risk for money laundering and/or financing of terrorism. Areas that are known to have high crime rates and/or are located in border areas between countries potentially have higher PU/PT risks. Country of origin/destination of the transaction known to have low APU & PPT compliance rate also has high PU/PT risk. Country and geographical area is also one of the parameters in SRA, so the result of CFS is the main reference in determining the parameters of assessment of the level of a Operator's geographical risk as follows:

| Parameter | Non-Bank MVTS | Non-Bank Money Changers |
|---|---|---|
| Business Location | Number of business locations in Jakarta, East Java, Jakarta, Central Java, and others. | Number of business locations in Kepulauan Riau, Bali, and others |
| Country of origin/ destination of transaction | Volume and Nominal transactions of origin/destination of | N/A |

| | | |
|---|---|---|
| | transactions for North Korea, Iran, Syria, Myanmar, Afghanistan, Sudan, Cuba, British Virgin Island, Cayman Island, Nigeria and others. | |

c. Product/Service Risk

Products and/or Services offered by the Operator have the potential to be used in money laundering or terrorism financing activities. Risk assessment of products and/or services is performed using the mechanism parameters, values, volumes, and transaction types. The data must be prepared by the Operator in the form:

| Parameter | Non-Bank MVTS | Non-Bank Money Changers |
|---|---|---|
| Transaction Mechanism | • Total Transaction Nominal<br>• Cash-to-Cash Nominal Transaction | • Total Transaction Nominal<br>• Cash-to-Cash Nominal Transaction |
| Transaction composition | Nominal amount and volume of incoming, outgoing, and domestic transactions | Nominal amount of transaction for sale and purchase of USD, SGD and other currencies |

d. Transaction networks

Transaction network is media of transaction implementation of a product or service. High risk is attached to the distribution network that allows for transactions without going through a face-to-face process with service users, such as transactions that are fully done online. This risk may also arise and the number of service points/branch offices in the country, as well as the number of partners inside and outside the country. The more number of service points/branch offices and number of partners increases the risk level due to the increased risk of non-compliance with the provisions of the APU and PPT, and the

increasing need of the Operator's control over the point of service and/or partners. The data must be prepared by the Operator in the form of:

| Parameter | Non-Bank MVTS | Non-Bank Money Changers |
|---|---|---|
| Number of service points | Number of service point | Number of service point |
| Cooperation partner | Number of partner | Number of partner |

After collecting the data, the Operator must calculate the value of its inherent risk by entering data on too/RBA prepared by BI (Appendix 1 Risk Assessment Form) V Risk values divided into 3, i.e. low, medium and high).

| Low | Medium | High |
|---|---|---|
| Description:<br>Operators are exposed to TPPU & TPPT risks but are low<br>Action:<br>Operators run PBI APU & PPT as well as adequate monitoring. | Description:<br>Operator exposed to risk of TPPU & TPPT of medium scale.<br>Action:<br>Operators undertake monitoring efforts and efforts to prevent increased risks. Example: socialization of regular employees regarding APU & PPT implementation guidelines. | Description:<br>Operator exposed to high risk TPPU & TPPT.<br>Action:<br>Operators make special and maximum efforts to implement more stringent risk mitigation in order to minimize such risks. Example: application of transaction limit on cash transaction |

2. Assessment

The Operator then self-assesses the application of the APU & PPT program to assess compliance with applicable provisions by answering the questionnaire on the Self-Assessment form provided by BI (Attachment 2 of the Self-Assessment Form).

Assessment is based on Operator's compliance with aspects of: (a) Active supervision of the Board of Directors and Board of Commissioners; (b) written policies and procedures; (c) Risk Management; (d) Internal Control of Human Resources.

The assessment criteria are as follows:

| FINAL SCORE | PREDICATE |
|---|---|
| 1-1.99 | Very Good |
| 2-2.99 | Good |
| 3-3.99 | Quite Good |
| 4-4.99 | Not Good |
| 5 | Poor |

3. Control

The control stage is the stage to make improvements to the results of self-assessment. Operator must cover the deficiencies in the five aspects of compliance above. For example, if the Operator has not provided APU & PPT training to the employee, the Operator must immediately provide training to the employee.

If the Board of Directors has not given approval to the SOP of APU & PPT implementation, the Board of Directors must immediately establish the latest SOP and sign together with the commissioner,

4. Risk Mitigation

a. Risk mitigation planning and implementation

At the risk identification stage, the Operator may asses the risks on its business. Therefore, the Operator shall determine and implement the actions to deal with such risk, for example:

- the operator only serves cash-to-cash transactions. Therefore, the operator must apply a maximum limit of transaction amounting to Rp25 million.
- Operator has 20 service points spread across several provinces in Indonesia. To ensure all employees understand and be able to apply SOP properly, then Operator holds the employee knowledge refreshment once every 3 months. The APU & PPT work unit at the head office carries out monitoring of the correctness of user service user data inputs at all points of service on a regular basis,
- Monitoring and evaluation of implementation of risk-based approaches.

Operator should monitor the implementation of a risk-based approach in the implementation of the APU and PPT Operator programs. Monitoring of risk management implementation is carried out by the responsible work unit in the implementation of APU & PPT program. Furthermore, the monitoring results shall be reported to the Board of Directors and Commissioners so that they can perform their duties to oversee the implementation of APU & PPT programs. Operator must reevaluate risk identification, mitigation, procedural policy, and internal control if there is a change of structure and scale of business activities and the development of new products.

## D. Human Resource Management

Human resource management, shall at least include:

1. Pre-employee screening; The Operator is obliged to screen the prospective employee among others ensuring that the prospective employee is never involved in the PU/PT activities and by comparing the identity held with DTTOT.
2. Employee profile monitoring:

Operator must always monitor the employee profile including profiling identity data and employee competency.

3. Continuous employee training and awareness improvement programs.

   There are several methods to increase knowledge of APU and PPT to employees, e.g. through discussion, workshop, training, self-learning, e-learning and so on. For example, Employees may obtain knowledge on PAU and PPT through the PPATK and Bank Indonesia Website. Training and understanding programs must be implemented on a regular basis as evidenced by official events/programs and attendance lists signed by employees who have participated in training/sharing knowledge.

E. Internal Control

Internal control systems, shall at least include:

1. The Operator shall have a function responsible for the application of APU & PPT. Designated functions should be tailored to the business scale of the Operator, which may be in the form of a work unit or by appointing directors/executive officers to be in charge of the implementation of the APU & PPT program.

   The formation/assignment of the responsible persons of APU & PPT is followed by written documents, including the Directors' Decree which designates the names and job descriptions of PPU PPT officers; inclusion of APU PPT officer name in SOP APU PPT; inclusion of name of person in charge, liaison, and reporter on registration GRIPS-PPATK.

2. If there is an audit function in the Operator, there shall be a clear separation of duties and authority between the units acting as an internal audit with the Operator's business units.

3. The operator shall periodically be required to be audited with an independent party (external party or independent party within the company) in accordance with the business scale of the Operator).

4. Reporting

The Operator shall comply with routine reporting in the provisions to be reported on schedule determined by both routine and incidental reports requested by the regulator.

a. Report to BI:

1) Report of policy changes and written procedures of application of APU and PPT maximum of 10 days from change)

2) Annual APU & PPT application report (maximum January next year) BI provides report format in Annex 3 (Annual Report on APU & PPT Program Implementation).

3) Reports on freezing of transactions, account freezing, and/or denial of transactions related to DTTOT and list of funding of proliferation of weapons of mass destruction (maximum of 10 days from the act).

4) Other reports.

b. Report to PPATK:

1) LTKM

2) LTKT

3) LTKL

4) Other reports

5. Information System and Data

Given the complex nature of the RBA process, Operators require special applications to be able to monitor, especially for Operators with complex business scales (among other things indicated by the number of service points, transaction types, service users, number of products, currency type, large geographical area). To facilitate data processing operators who currently do not have a special application, BI provides a spreadsheet format. But this requires the discipline of the Operator to be able to implement it effectively.