SUPERINTENDENCY OF BANKS OF PANAMA
PREVENTION & CONTROL OF ILLICIT OPERATIONS DIVISION
GUIDELINES FOR THE IMPLEMENTATION OF THE RISK-BASED APPROACH
SECTOR: TRUST SERVICE PROVIDERS • VERSION: 1 • SEPTEMBER 2019

Superintendencia de Bancos de Panamá

These guidelines were intended to provide a non-binding reference for the effective implementation of the risk-based approach for Anti-Money Laundering, Countering the Financing of Terrorism and Proliferation of Weapons of Mass Destruction (AML/CFT/WMD) methodology for Trust Service Providers (TSP) in the Republic of Panama.

The implementation of the Risk-Based Approach (RBA) model by the Reporting Entity (RE) must be developed through the analysis, implementation, and authorization of the Anti-Money Laundering Committee (AMLC), or the Board of Directors (hereinafter referred to as Top Management or TM) in case of not having a committee. This should always be done based on the proposal of the Compliance Officer (CO) or the individuals appointed by the AMLC or TM. Therefore, the entire development and implementation mechanism must be conducted collaboratively within the RE.

To implement the RBA for AML/CFT/WMD within the RE, at least the following elements of the model should be considered (see Figure 1).

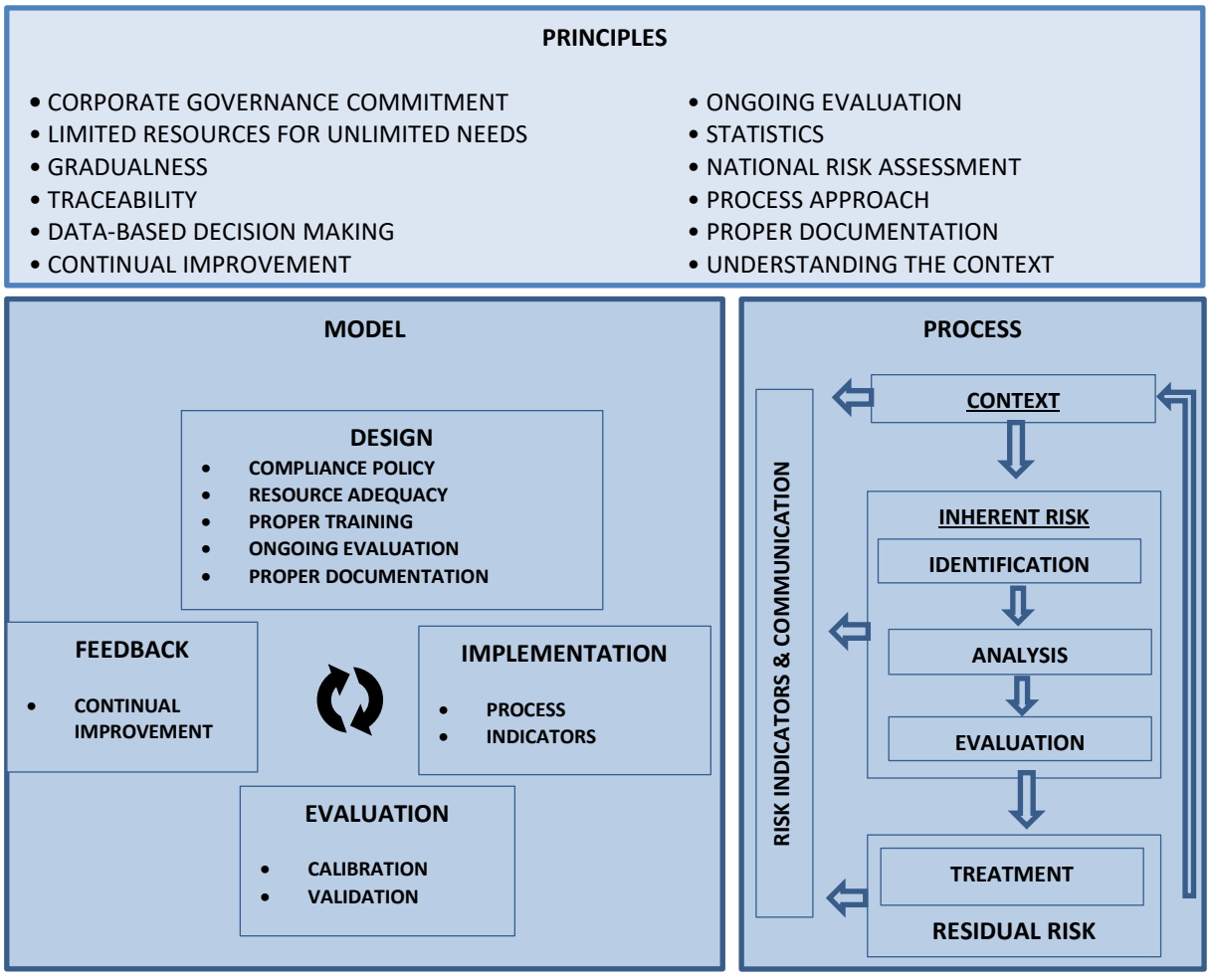


Figure 1

SUPERINTENDENCY OF BANKS OF PANAMA
PREVENTION & CONTROL OF ILLICIT OPERATIONS DIVISION
GUIDELINES FOR THE IMPLEMENTATION OF THE RISK-BASED APPROACH
SECTOR: TRUST SERVICE PROVIDERS • VERSION: 1 • SEPTEMBER 2019

Superintendencia de Bancos de Panamá

RBA FOR AML/CFT/WMD PRINCIPLES

PRINCIPLES

- CORPORATE GOVERNANCE COMMITMENT
- LIMITED RESOURCES FOR UNLIMITED NEEDS
- GRADUALNESS
- TRACEABILITY
- DATA-BASED DECISION MAKING
- CONTINUAL IMPROVEMENT
- ONGOING EVALUATION
- STATISTICS
- NATIONAL RISK ASSESSMENT
- PROCESS APPROACH
- PROPER DOCUMENTATION
- UNDERSTANDING THE CONTEXT

To better understand the RBA for AML/CFT/WMD, we will begin by defining the risk of Money Laundering, Terrorist Financing, and Financing the Proliferation of Weapons of Mass Destruction (**MLR** or **Money Laundering Risk**). The **Money Laundering Risk** is the possibility and likelihood that a criminal group uses the RE to commit crimes or to conceal, disguise, or hide the source of income, or its use thereof, for criminal activities included in Panamanian legislation as predicate offenses to ML/TF/WMD.

The **MLR** is also defined as the likelihood of loss or damage that a RE may suffer due to its exposure or propensity to be directly or indirectly used as an instrument for money laundering and/or channeling resources toward terrorist activities, or when concealing assets originated or destined for those activities is intended.

The **MLR** materializes in REs through various associated risks, such as operational risk, reputational risk, legal risk, and more. The handling and processing of these risks are the responsibility of the entire organization. The principles that REs should consider when designing, evaluating, and implementing [the RBA] are listed below:

- **Corporate Governance Commitment.** Top Management and corporate governance should clearly and objectively establish their unconditional support for compliance with and understanding of the risks related to **MLR**. This commitment is demonstrated by implementing effective measures to ensure the functioning of the **Risk Management Model** and **Process**. All actions and measures should be documented to demonstrate their ongoing commitment to fulfilling any requests from the Superintendency of Banks of Panama (SBP) or the competent authority in this matter. It is important to note that this approach follows a Risk-Based Approach rather than a regulatory compliance checklist.

- **Limited Resources for Unlimited Needs.** Managing and addressing various requirements and needs for risk management becomes a challenge due to limited resources. To effectively tackle this issue, it is essential to identify the level of risk to which the RE is exposed. The effective allocation of the RE's or customer's risk rating demonstrates the principle of **Limited Resources for Unlimited Needs**. **Corporate Governance** should demonstrate the maintenance of validated methodologies and calibrated

tools for effectively rating the risk of both customers and the RE. The statistics and results of ongoing evaluations must be familiar to the AMLC or TM and should be presented by the CO.

- **Gradualness**. Gradualness can be exemplified as follows: **the greater the risk, the greater the due diligence**; therefore, **the lesser the risk, the lesser the due diligence**. The gradual nature of the **Money Laundering Risk** posed by the commercial relationship with a customer or potential customer is key to effectiveness. The RE should adequately establish a model for rating the customer's and RE's risk (with prior authorization from the AMLC or based on the CO's proposal). This model should be based on statistical models tailored to their needs and reflecting expected statistical behavior.

- **Traceability.** The ongoing and timely monitoring of operations, information, data, transactions, channels, products, activities, and other relevant information of a customer or potential customer is key to the RBA. The RE should comprehensively monitor all data, operations, movements [conducted by the customer], and other information [provided by] the customer. This monitoring should go beyond considering only the agreement, service, internal control, or follow-up model conducted by the entity for controlling or accounting purposes. The **traceability** of operations should always be linked to the customer. Any other practice by the RE would not be effective for the purposes of a proper RBA.

- **Data-Based Decision Making.** Evidence is the foundation for certainty and proper risk management. The RE should consider permanently documenting the decisions made within the RE, whether by the AMLC, the TM or through the legal authority of the CO, as best practices. Model effectiveness is based on demonstrating to the SBP, with supporting documents, that the RE understands the ML/TF/WMD risks to which it is exposed. The RE must ensure that it takes the necessary measures to effectively mitigate these risks and must also demonstrate why it assigned a specific risk rating to a customer, detailing the considerations the CO documented regarding whether to report an operation, with prior authorization from the AMLC or TM, or explaining why the RE made one decision over another. The RE should also have a clear narrative explaining why it took a certain action or refrained from doing something at a specific time, always following the principle that **"if there is no evidence, it did not happen."**

- **Continual Improvement.** Enhancing risk assessment models represents a vital commitment to **Corporate Governance** in the context of AML/CFT/WMD. This enhancement stems from the ongoing review and self-assessment program. The context is changing, and the models are seasonal, making it imperative for the RE to maintain documentary evidence of the revisions and enhancements applied to the **RBA model** for a minimum of 5 years. This evidence should encompass statistics and the outcomes of their implementation.

- **Ongoing Evaluation.** The context and risks for the RE are dynamic. The RE should regularly adapt its risk assessment tools to both the entity and its customers. This adjustment should take place at least once every six months or whenever a new branch, new product, or new channel is introduced, or when there is a substantial change in the customer's transactional behavior.

  When operating conditions change and the review reveals that the customer's expected statistical behavior is not present, the RE should adjust its risk assessment models. If the model fails to effectively distinguish and evaluate customers who were assigned high-risk ratings from those with different risk ratings, the RE should have a testing model in place to perform effective calibration of the customer risk assessment tool. Additionally, the RE should possess evidence of these tests to demonstrate their efficacy.

- **Statistics.** The customers of the RE constitute a target audience from a statistical perspective. The RE should establish effective models to categorize its customers based on their characteristics, such as activity, transactional level, country of origin, products they engage with, or any other characteristic or combination of characteristics that enable clear and effective differentiation among various groups within the risk ratings established by the RE. The statistics should be defined by the AMLC or TM, with the proposal of the CO, and they should remain consistent across each fiscal year. This consistency is important for valid comparisons between different months of the year or under comparable criteria during the year, in alignment with the customer's economic cycles.

  The statistics should enable the RE to demonstrate that there is mobility among customers with the assigned risk rating and that proper customer segmentation is consistently achieved. It is recommended to consider the following statistical models within the RE's Risk-Based Approach (RBA):

  1. **Statistical Correlation.** A statistical correlation must exist between the risk rating assigned by the RE and customer transactions. Here, transactions refer to the actual inflow and outflow of resources and/or assets to or from the trust. Refer to Figure 2.

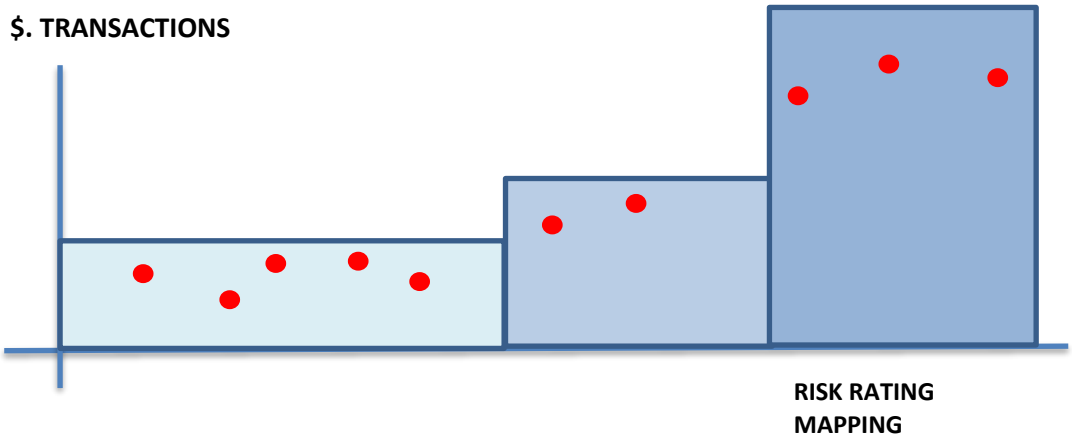


Figure 2

2. **Pareto Principle and/or Standard Normal Table**. The RE should demonstrate the effectiveness of its customer risk rating mapping through a statistical analysis. The RE must have distinct high, medium, and low risk ratings as applicable. It should also show that its target audience exhibits an expected statistical behavior, supported by relevant documentation. The statistical demonstration must effectively differentiate those with the highest risk from those with the lowest risk. This can be summarized as follows: out of 100% of current customers, the tool segregates individuals representing greater risk from those assigned high risk ratings based on the **statistical correlation**, and those representing lower risk are assigned lower risk ratings. Please refer to Table 1.

Statistics Model	**Risk Level**	**Percentage of the Target Audience Included**
PARETO	HIGH (customers rated with the highest risk rating)	4.00%
	MEDIUM (customers rated with a medium risk rating)	16.00%
	LOW (customers rated with the lowest risk rating)	80.00%
STANDARD NORMAL TABLE	HIGH (more than 2 standard deviations)	2.28%
	MEDIUM (target audience between 1 and 2 standard deviations)	13.59%
	LOW (less than 1 standard deviation)	84.13%

Table 1

The RE must demonstrate that the application of the customer risk rating tool is operational and validated through a statistical technique. The risk matrix is a tool for assessing a target audience; the RE could employ the

Z-table, standard normal table, Pareto, or another model that facilitates the calibration of measurement or evaluation instruments. The choice of tool or model should be contingent on factors such as the size of the target audience, integrated variables, and weightages. For consistency, a model can only be changed when the methodology itself is being validated.

- **National Risk Assessment.** Panama periodically conducts a National Risk Assessment (NRA). In the NRA, REs become informed about areas with vulnerabilities that pose specific concerns for the country on a given date. The RE should effectively demonstrate that it has taken the criteria and findings of the NRA into account while designing its risk assessment tools. Under no circumstances should the risk rating assigned by the RE for a variable or criterion be lower than the rating assigned by the NRA to the event or indicator at a national level. The AMLC or TM is responsible for ensuring coherence between the risk ratings assigned in the NRA and those assigned within the RE. These evaluations and verifications should be documented in the AMLC or TM meeting minutes.

- **Process Approach.** The RE should comprehensively document all its processes to ensure operational certainty. For example, there may be information generated by the Operational or Commercial department where the Compliance Area (CA) acts as a user. If the information input into the database is incomplete or inaccurate, it will lead to errors in risk rating. An effective customer risk rating cannot be achieved if the source of information fed into the tool is incomplete, inaccurate, contains visibly erroneous data, or lacks temporary validity.

  The effectiveness of customer risk rating directly depends on the quality of the data. Therefore, the RE should clearly define **Corporate Governance** responsibilities and demonstrate commitment to providing accurate information to the CA for effective customer or user risk rating. The RE should comprehensively document and understand the impact of the compliance model processes that generate information and ensure its effective utilization, as depicted in Figure 3.

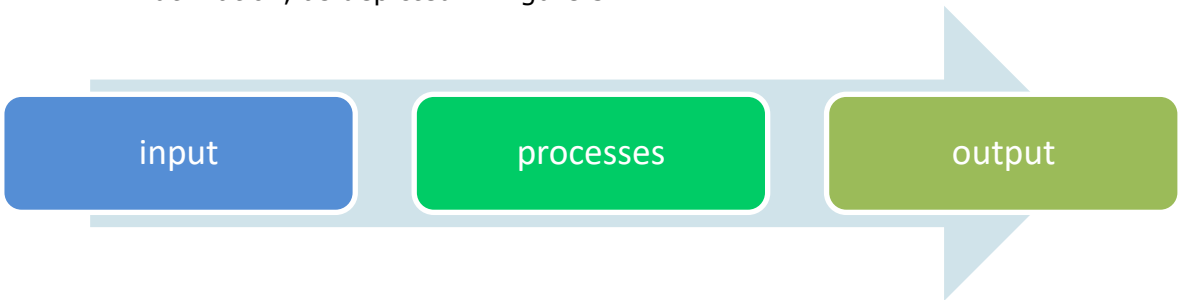


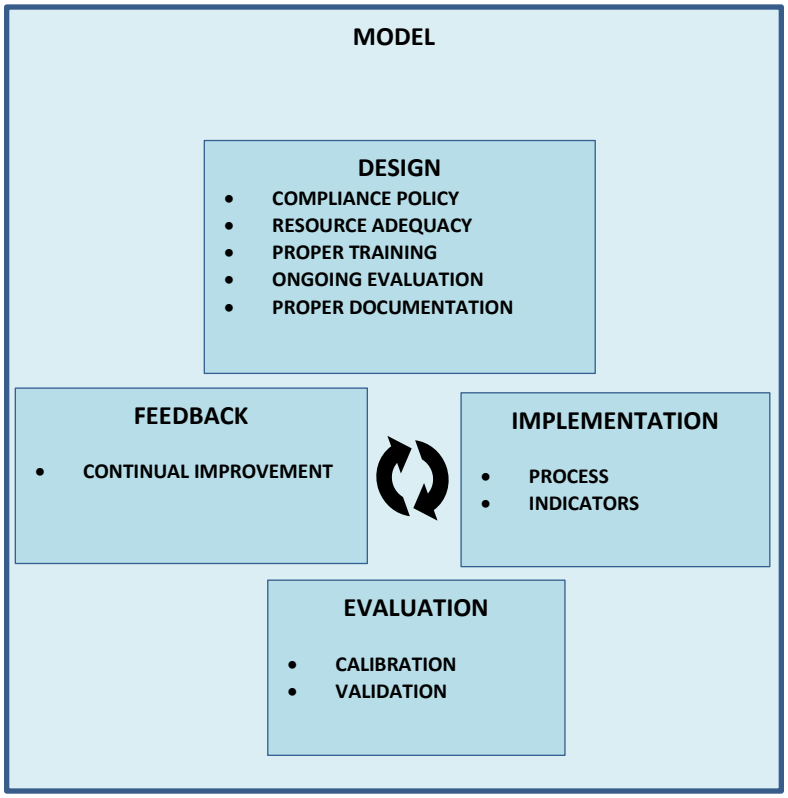
Figure 3

- **Proper Documentation.** The RE should thoroughly document its processes to demonstrate the effectiveness of the model. Documentation within the CA can be developed across various areas or departments of the RE. Therefore,

the CO should maintain a list of documents, processes, procedures, models, files, and other evidence to clearly identify their roles in the RE's regulatory compliance. The RE can retain both digital and hardcopy documents, images, and other forms of evidence, provided they are accessible for evaluation by the SBP to assess their effectiveness and relevance in ensuring compliance with the applicable regulations.

- **Understanding the Context.** The RE should document the rationale behind assigning a high-risk rating to a particular risk, criterion, factor, or indicator. If the RE decides to include a criterion due to its unique characteristics or to exclude one that is not deemed significant for specific reasons, the RE must thoroughly document these decisions. The document should be self-descriptive and made available to the SBP to facilitate effective offsite and onsite examinations. The '**Understanding the Context**' document must serve as the methodological support and explanation of the **RBA model and process**. Its creation is the sole responsibility of the CO, under the supervision of the AMLC or TM, and evidence of its submission and authorization by the **Corporate Governance** should be present.

RBA FOR AML/CFT/WMD MODEL



The RBA for AML/CFT/WMD model consists of 4 phases, which are described as follows:

DESIGN

Within the **Design** phase, the RE should have the following documented elements, as a minimum, to clearly demonstrate its methodology for implementing the RBA for AML/CFT/WMD. In all cases, the RE should demonstrate that it has addressed each of the following topics:

- **Compliance Policy.** The RE should effectively communicate the AML/CFT/WMD Compliance Policy to all its employees. This Policy should be defined in internal documents, expressed clearly, and subject to ongoing evaluation to assess its alignment with the established objectives. The **Compliance Policy** is an integral part of the methodology and must be internally disclosed. The **Corporate Governance** should explicitly define and unmistakably declare its commitment to adherence. The RE should document its approach to maintaining the **Compliance Policy** up to date, including review periods and grounds for potential updates.

- **Allocation of Resources.** The RE and its **Corporate Governance** should demonstrate compliance with the **Compliance Policy** by effectively allocating relevant resources for its activities. The **Corporate Governance** should reliably and directly exhibit the allocation of necessary and pertinent resources to demonstrate model effectiveness. Requests for resources from the CO, the AMLC, TM, and other involved departments should be documented, whether authorized or not, to highlight the efficacy in designing the **Compliance Policy**. When designing the model, the RE should document how it will ensure coverage of resource needs, identifying those to be met during the fiscal year and those deferred to other fiscal periods due to budgetary constraints.

- **Proper Training.** The RE should demonstrate that the personnel from different areas with direct responsibility for AML/CFT/WMD compliance have received effective training for performing their duties, including the **first line of defense**. The RE should provide documentary evidence that all personnel in the CA, and as a minimum, those in Internal Audit and Risk Management, have received the necessary training for the proper execution of their tasks. When designing, the RE should outline how it will ensure the suitability of involved personnel for their roles and how it will maintain their efficiency in the face of new technological challenges, platforms, or operating environments exposed to **MLR**.

- **Ongoing Evaluation.** The RE should demonstrate the presence of measurement mechanisms or techniques that enable continuous monitoring of **MLR**. The RE should establish performance indicators for issues responsible for effectiveness, such as the percentage of incomplete high-risk customer files, the number of customers with incomplete nationality data,

update time of high-risk customer files, percentage of customers rated as high-risk, percentage of customers rated as low risk, among others. The RE should clearly define its approach to measurement and frequency to maintain a perpetual evaluation model enabling immediate corrective actions upon detection indicators falling outside acceptable parameters.

- **Proper Documentation.** The RE should physically or digitally document, as per responsibility, manual type, hierarchy, position, function, or user type, whichever is deemed pertinent. This documentation is necessary to ensure effective performance of responsibilities and functions. It is important that the RE maintains a printed compilation of all in-force documents and monitors various versions of documentation used or previously used for AML/CFT/WMD compliance. The RE should refer to this documentation compilation as the **Anti-Money Laundering Manual** (**AMLM**). It should encompass all documents, formats, writings, and other references necessary to comply with applicable legal obligations, regardless of the performer. The scope, objective, reference standards, process or use assigned to them should be permanently and clearly established. Furthermore, issuance date, revision number, and any pertinent control information as deemed necessary by the RE should be included.

IMPLEMENTATION

To achieve an effective implementation of the **model**, the RE must possess a suitable **process** (refer to **Process**) that aligns with the reporting entity's **Compliance Policy**. The RE accomplishes this by adhering to the aspects outlined below.

- **Process.** The RE must develop an RBA methodology (refer to **Process**), which should include the following elements, as a minimum: **Context** analysis; **Inherent Risk** Identification through risk **Identification, Analysis, and Evaluation**; risk **Treatment**; and, consequently, the calculation of **Residual Risk**, along with **Risk Indicators** and **Evaluation**. The RE should clearly establish, in conjunction with its **Compliance Policy** and **Corporate Governance**, mechanisms for effectively designing the **Process**. The CO, initially, and subsequently the AMLC or TM, are the key parties directly involved in the design. However, the application and development are the responsibility of the entire RE.

- **Indicators.** The RE should establish risk indicators. In all cases, it should clearly define the risk rating at the time of evaluation, determine the ideal risk rating, its tolerated risk, its **Inherent Risk** indicators, and the result after treatment as **Residual Risk**. The RE should demonstrate its commitment to first address the most critical **Inherent Risks**, considering both the likelihood of the risk event and the expected economic impact. The indicators can be determined using the ***LIKERT*** scale, absolute terms, or indicators established by the RE itself. It is recommended to create **Inherent Risks** and **Residual Risks** heatmaps to graphically illustrate the existing risk exposure and expected improvements to the RBA.

EVALUATION

To demonstrate the effectiveness of the model, the RE must conduct ongoing evaluations of the model. Therefore, it is crucial to undertake two evaluation phases:

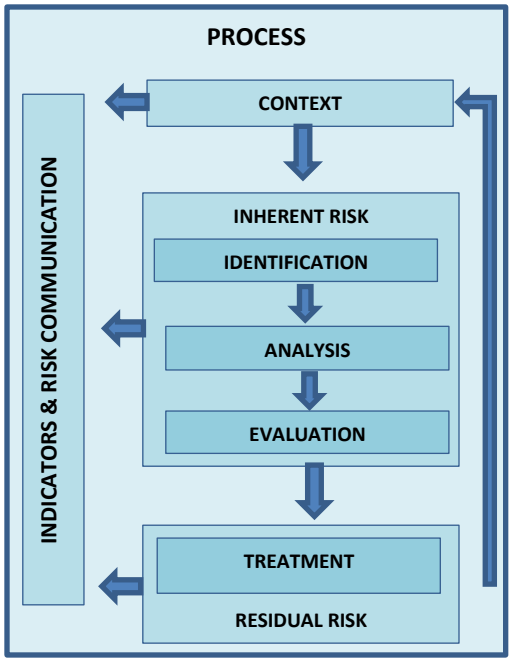
- **Validation.** The RE should conduct validation of the **RBA model** at least once every twelve months, which is equivalent to at least once a year. The AMLC or TM, upon the recommendation of the CO, must seek authorization from **Corporate Governance** to continue using the implemented methodology or, if necessary, propose improvements that effectively demonstrate the adequacy of the **model** based on the RE's characteristics. The RE must maintain evidence of the review conducted for each aspect, including the rationale behind changes and both quantitative and qualitative demonstrations of their effectiveness. In all cases, the RE should establish that the **RBA model** can be adjusted as needed due to operational conditions.

- **Calibration.** The RE should establish a **Calibration** process for the risk rating tools used within the organization, both for the Entity's risk evaluation as well as the customer risk rating tool. The RE should incorporate the **Statistics** principle into its reference documents. Furthermore, the RE should demonstrate the effectiveness of the tools it employs in accurately discerning and evaluating the **Statistical Correlation**, as well as the outcomes derived from the evaluation of the **Pareto Principle** and/or **Standard Normal Table**.

FEEDBACK

Continual Improvement. The continuous application and evaluation of the **RBA model** by the RE result in **Continual Improvement**. The RE should clearly define the frequency and responsible parties for conducting independent evaluations of the model's effectiveness. These independent evaluations should be performed by individuals possessing the necessary training to comprehend the applied methodologies and accurately interpret evaluation results. It is recommended that evaluations cover periods of one year or less. Independence in this context means that there must be no conflict of interest between the evaluator and the entity being evaluated. Any form of pressure to withhold or disclose information must be documented in the report by the independent auditor or communicated to the SBP through written documentation.

RBA FOR AML/CFT/WMD PROCESS



To properly develop the **process**, the RE should establish mechanisms for maintaining continuous monitoring across various aspects, which include:

CONTEXT

Context. Within the **process**, the RE should clearly define who will be responsible for and how frequently the operational conditions, upon which the **model** and **process** were **designed**, will be verified. This encompasses examining changes and ensuring that reference standards or laws, market-offered products, distribution channel conditions, customer transaction amounts, or any other factors that may undergo modification over time have remained consistent. The RE should document the assigned responsibilities and the mechanisms it intends to employ to ensure the effectiveness of the **context** monitoring model.

Within the **context**, the RE should establish mechanisms to both incorporate and exclude variables as necessary and subsequently recalibrate the **statistics**.

INHERENT RISK

Inherent Risk is the evaluation of the likelihood and economic impact at the time of assessing risk events. Within the **process**, the RE shall establish criteria for determining the value of likelihood or economic impact of the **risk**. The RE should determine the **Inherent Risk** using either statistical analysis or expert judgment (both approaches must be validated by the AMLC or TM). These approaches should consider

the current values for determining the **Inherent Risk**, encompassing at least the following topics:

Identification. The RE should establish at least four risk categories for the RBA for AML/CFT/WMD (in the case of other risks, they may be more), which are, as a minimum:

1. **Customer**
2. **Geography**
3. **Product**
4. **Transactional Level and Distribution Channel**

In all cases, the RE should consider these four **Risk Categories** as a minimum. Once the **risk categories** are determined, the RE should establish the relevant **Risk Factors** for their evaluation. For example:

1. **Customer**
   a. Activity, purpose and/or source of income.
   b. Age of the business or legal entities participating in the trust.
   c. Age of the trust agreement.
   d. Economic sector to which it belongs.
   e. Telephone number.
   f. [Legal] Representative's e-mail address.
   g. And others.

2. **Geography**
   a. Nationality of the parties, of the legal arrangement, etc.
   b. Origin of the resources that will be incorporated into the agreement.
   c. Destination of the resources where the flows produced by the agreement will be sent.
   d. Country of incorporation of the trust agreement.
   e. Operational address or domicile where the existence of the purpose of the agreement can be verified.
   f. And others.

3. **Product**
   a. Comparison between various trust products or types of services to determine which is more prone to **Money Laundering Risk**.
   b. Other criteria.

4. **Transactional Level and Distribution Channel**
   a. Comparison between channels used in the administration of the agreement to determine which is more prone to **Money Laundering Risk**.
   b. Transactional amount, including in-kind contributions.
   c. Customer or agreement operation channels.
   d. Monetary instruments used for transactions or the type of assets involved.

e. Transactional frequency, including for non-operating trusts (custody of assets).
f. And others.

ANALYSIS

The RE should assign a weight to each **category** and assign relative importance to each **factor** within the **category**. This is why the RE should establish within its methodology and **process** the mechanism it will use for risk rating, including the various weights and specific factors, and what the expected result of the application is.

The RE should clearly establish the criteria for allocating weights and ensure that the methodology review exercise is analyzed, evaluated, and authorized by the AMLC or TM. The **Corporate Governance** must be informed of the results and conformity of the models applied to its customers. The CO and the AMLC or TM are responsible for ensuring that the model used is effective for the target audience and that the tool used is calibrated to ensure effective risk rating.

The sum of the allocated or weighting scores must always add up to 100%. If the RE determines that some variables are not applicable to it due to substantiated considerations, it may assign a minimum value to the **risk category** or to some specific **factor** (e.g., that of customer when the resources are provided by the Government of the Republic of Panama). The result of applying a value to a **factor** or **category**, for customers or for a target audience, should be variable, i.e., dependent on customer characteristics. The value assigned to a variable must be sensitive to differences. If the value obtained by all customers is the same, it will be justified as a constant in the target audience. For that **factor** or **category** (as appropriate), a minimum value may be assigned to ensure it does not disproportionately affect other factors. The RE must always have, at least, the four **categories** identified: **Product**, **Customer**, **Geography**, and **Transactional Level/Distribution Channels**.

The rationale for the inclusion and value of the **categories** and **factors** is the analysis process, the tool design, and other topics that are included or minimized for statistical reasons. This documentation should be prepared by the CO and communicated to the AMLC or TM.

When it comes to trusts where the funds are provided by Government agencies or institutions, even when the signatories are Politically Exposed Persons, the RE may apply the low-risk criterion if there are no other factors that, when analyzed, change the risk rating. When the RE substantiates the application of the criteria for simplified file integration or the low-risk rating of the trust within its internal documents or **AMLM**, these criteria must be clearly defined for management and identification purposes. As a result of the risk assessment, this risk rating may be assigned when the economic contributions have a certain source and originate from government resources.

There are relevant factors within trusts. In cases where the parties or decision makers are not evident, the identification of the beneficial owner, the signatories, the contributors, and other parties to the trust must be conducted. It should be noted that

the onboarding criterion depends on the parties who contribute the highest risk rating to the commercial relationship among all the signatories and parties to the agreement.

All trusts have an economic purpose, whether it involves the administration of assets and patrimonial resources, custody of valuables, administration of public resources, etc. In the **transactional level/distribution channel**, any economic or in-kind contribution that result in a change in the amount managed or safeguarded by the trust will always be evaluated as a **transaction**. The rationale of the monetary instrument and other characteristics of the contribution of assets, whether monetary resources, rights, or securities given to or withdrawn from the trust, should be considered in terms of **transactional level**.

EVALUATION

The RE should have properly documented the application of the criteria for impact and likelihood in the calculation of **Inherent Risk**. In all cases, the AMLC or TM and the CO are responsible for implementing the model. The CO must present the rationale and raise awareness among personnel and employees in **First Line of Defense** about the importance of having accurate, timely, clear, and data-based information. The CO must ensure that when information is input into the risk assessment tool, it results in a value within a range agreed upon and known by the AMLC or TM and the CO. The evaluation and its result could be represented in a heatmap.

The RE should clearly establish the criteria for prioritizing risks based on the calculation of **Inherent Risk**. In all cases, the treatment and priority should have a reasonable justification, and the determination of the evaluation criteria should be documented clearly, objectively, and precisely.

RESIDUAL RISK

TREATMENT

The **RBA models** address two important aspects: **Risk Mitigators** and the **Decision-Making process**. In both cases, the CO and the AMLC or TM are personally responsible for making decisions about the risk and the development of **mitigators**. As examples, the following are introduced, in an illustrative but not limiting manner, as **Money Laundering Risk Mitigators**.

- **Processes.** The RE should properly establish the design, development, and implementation of relevant processes to maintain an acceptable risk level, both due to customer risk evaluation and the risk associated with AML/CFT/WMD. These processes include documents, formats, documented procedures, and any other document, data, hardcopies, or digital information that are established to control the way specific activities are performed.

- **Training.** The RE should establish relevant **training** processes for the Commercial and Control areas, as well as all those areas in which important activities are to be performed within the AML/CFT/WMD process. **Training** is

intended to provide the necessary skills to the personnel responsible for the **processes**, enabling them to have the necessary mechanisms, criteria, experience, and sensitivity to identify the importance of their activities within the AML/CFT/WMD [measures]. In all cases, it is recommended that staff receive not only training but also skill development.

- **Monitoring/Technology.** The RE should establish appropriate mechanisms to effectively monitor **Money Laundering Risks**. Monitoring includes continuous database measurement, model evaluation, operational monitoring, customer transactions, the technological infrastructure necessary for monitoring, effective computer systems, parametrization of red flag systems, follow-up and treatment of red flags, and other indicators.

- **Supervision/Audit.** The RE should establish mechanisms to verify the correct performance of **processes**, **training**, **monitoring/technology**. The establishment of adequate performance indicators in the **monitoring/technology** area is important for effective supervision. The **Audit** function should be independent from the area that manages commercial relationships and customer or user service. Internal **Audit** must be independent to oversee the models. Additionally, there must be external audits for a comprehensive evaluation. The RE should ensure the relevance of the audit model, as well as the skills and experience that the audit team must possess to effectively perform its duties.

  It is the responsibility of **Corporate Governance** to ensure that the internal or external **Audit** functions comply with the characteristics of independence, experience, and timeliness for correct performance and valid feedback on RBA development. It is recommended that an independent audit be conducted at least once a year, and the Internal Audit area or those performing the function within the RE should continuously monitor the plans and programs established in the area to identify gaps promptly and make adjustments or corrections within a reasonable timeframe, rather than waiting until the annual review is conducted.

  The RE should establish appropriate mechanisms for the effective implementation of the designed mitigators. These mitigators could be either individual or a set of mitigators necessary for effective risk mitigation. Within the mitigators, the RE should designate responsible individuals for their implementation, specify the implementation date, and, when feasible, include the cost of implementation.

  The RE should effectively manage all **decision-making processes**, considering the **Residual Risk Evaluation** and comparing the impact and cost of mitigators. The decisions that the RE could make based on the obtained results are:

  1. **Risk acceptance**
  2. **Risk treatment**

3. Risk transfer

The RE should clearly establish the criteria under which it will make each of the decisions, and these powers cannot be delegated without the authorization of the AMLC or TM and the **Corporate Governance**.

INDICATORS AND RISK COMMUNICATION

As a result of the **RBA process**, the RE should establish models to keep all its personnel informed about the risks to which they are exposed, the appropriate measures to make them known, and who will be responsible for informing about the risk indicators and other important facts in the **RBA dissemination** and the AML/CFT/WMD program. This communication process should include evidence of the training or model used to publicize and evaluate the impact on the staff with responsibilities in the commercial onboarding processes. The RE should clearly establish what it will do in case its employees repeatedly do not pass the evaluation, the opportunities that will be given to employees to pass the evaluation, and the criteria for passing the evaluation. The relevance of the content and the timing is the responsibility of the CO and must be approved by the AMLC or TM.

GENERAL CONSIDERATIONS OF THE RBA FOR AML/CFT/WMD

When the RE documents its **processes**, it should do so effectively, considering the characteristics of its trusts, the geographical areas where they operate, the rationale of the purpose of the agreement, the parties in the agreement, the products it uses, technological limitations, etc. When documenting the RBA, the RE should recognize that one of the fundamentals of the model is **Limited Resources for Unlimited Needs**. The **optimization** of resources is an important indicator of the model. The RE could develop compensatory processes for other mitigators when, due to budgetary constraints, it cannot implement the ideal model for mitigating **Money Laundering Risk**.

The RE could establish mechanisms, processes, controls, parameters, red flags, etc., depending on the RE's **Money Laundering Risk** assessment. Therefore, it may have mitigators based on the risks it has identified, if the **Risk Identification, Analysis, Evaluation, and Treatment** model is effective.

In the case of a **Financial Group** and if there are other operating licenses supervised by the SBP, a single **RBA model** may be developed for the **bank** and its subsidiaries, if the subsidiaries (in this case, the licensed trust service provider) only offer services to the **bank's** customers. This integration may be valid when the accounts and controls of the **bank** are the ones that conduct the monitoring, risk rating, and file integration. The foregoing is notwithstanding that the RE (TSP) also considers the type, structure, and assets transferred to the trust for its monitoring function.

The RE may develop a single **RBA for AML/CFT/WMD**, provided that the subsidiaries only offer services to the **bank** customers. Only through this process they market their products or services to parties who are not **bank** customers. In such cases,

the RE must conduct due diligence and integration of the identification of the Beneficial Owner.

The RE should have at least 3 risk assessment tools:

- **Entity Risk Assessment Tool**
- **Operational Risk Assessment Tool for AML/CFT/WMD**
- **Customer Risk Assessment Tool**

The RE should apply these guidelines to all the tools, according to the model used. The SBP could request, at any time within its supervisory powers, the validation, calibration, and other documents to demonstrate the conformity and effectiveness of the **RBA model** implemented by the RE.

The RE should have developed a computer system that enables comprehensive operational testing through a model that is the same as the one being programmed, with the same database and identical operating characteristics. The SBP will require access, capturing, and running of various tests to demonstrate the effectiveness of the computer system, the red flags model, accumulation, customer identification, operations follow-up and, in general, to demonstrate that the automated system performs the functions for which it was designed. The parameterization of the computer system is the responsibility of the CO, and the AMLC or the TM will ensure that the minimum operational characteristics are in place to be effective in **identifying, analyzing, evaluating,** and **mitigating Money Laundering Risks**.

The RE should understand the term "**transactional level**," as the inflow and outflow of money, assets, securities, rights, resources, or any other instrument of value accumulation that is assigned and administered by a trust. ***DO NO CONFUSE THE RESPONSIBILITY OF REPORTING AND MONITORING THE AGREEMENT WITH THE RESPONSIBILITIES ACQUIRED WHEN THE TRUST HAS AN ACCOUNT WITHIN THE BANK***.

Transactional level is considered the accumulated value of incoming and outgoing resources by any means and in any monetary instrument from or to the agreement, globally in each period. The RE cannot bypass the monitoring of trust transactions. The **Transactional level** conducted by customers of trust agreements should entail the analysis, including the information of account statements of the banks in which they maintain the operations, expert evaluation of in-kind contributions, market value of the contributed securities, and other value accumulation items that the RE deems pertinent. These allocation criteria must be documented in the **AMLM**.

The RE should consider that the **AML/CFT/WMD risk** is assigned to the agreement and its parties. This determination necessitates the establishment of accumulation controls for the monitoring, red flagging, and rating model of the transactional profile. This profile should always be accumulated per customer. It should be established that conducting AML/CFT/WMD processes by **product** is inappropriate, as all Trust Agreements pursue an economic purpose.

If you have any questions about the application and technical support for these guidelines, please refer to:

- ISO 31000:2018, Risk Management System
- ISO 9001:2018, Quality Management System
- Gaussian Distribution (also known as Gaussian Curve or Bell Curve)
- Standard Deviation
- Standard Normal Table (Z-table)
- Pareto Principle
- Calibration of Measuring Instruments for a Specific Target Audience
- Segmentation of a Target Audience or Set Theory