Insurance
Regulatory
Authority

Bima Bora kwa Taifa

IRA

AML / CFT Risk Assessment - Insurers

Mary Nkoimu ACII, AIIK, ACSI

Chartered Insurance Risk Manager

1

On the Agenda

Content:

1. Introduction
2. Risk-Based Approach
3. Risk-Based Approach Cycle
4. Identification of Inherent Risk
5. Risk Reduction Measures
6. Implement Risk Based Approach
7. Purpose of a Risk Based
8. Compliance Program

2

Introduction

Introduction

- Financial Action Task Force (FATF) requires countries and financial institutions to identify, assess and understand money laundering and terrorist financing risks they face and take appropriate action.

- Insurers should identify, assess and take effective action to mitigate the identified money laundering and terrorist financing risks.

- A risk assessment is the foundation of a proportionate risk-based AML/CFT framework.

- An insurer’s AML/CTF compliance program is based on the risk assessment.

3

Risk Based Approach

Definitions under RBA

- Risk based approach is the identification, assessment and understanding the ML/TF risks to which an insurer is exposed and taking measures commensurate to the identified risks in order to mitigate them effectively.
- ML/TF risk is a factor of:
  - ⇨ Threat - persons, object or activity with the potential to cause harm;
  - ⇨ Vulnerability – elements of a business that may be exploited by the threat or that may support or facilitate its activities; and
  - ⇨ Consequence - the impact or harm that may be caused.
- Inherent risk - the intrinsic risk of an event or circumstance that exists before the application of controls or mitigation measures.
- Risk management - is the process that includes the recognition of ML/TF risks, the assessment of these risks, and the development of methods to manage and mitigate the risks that have been identified.
- Residual risk - the level of risk that remains after the implementation of mitigation measures and controls.

Risk Based Approach

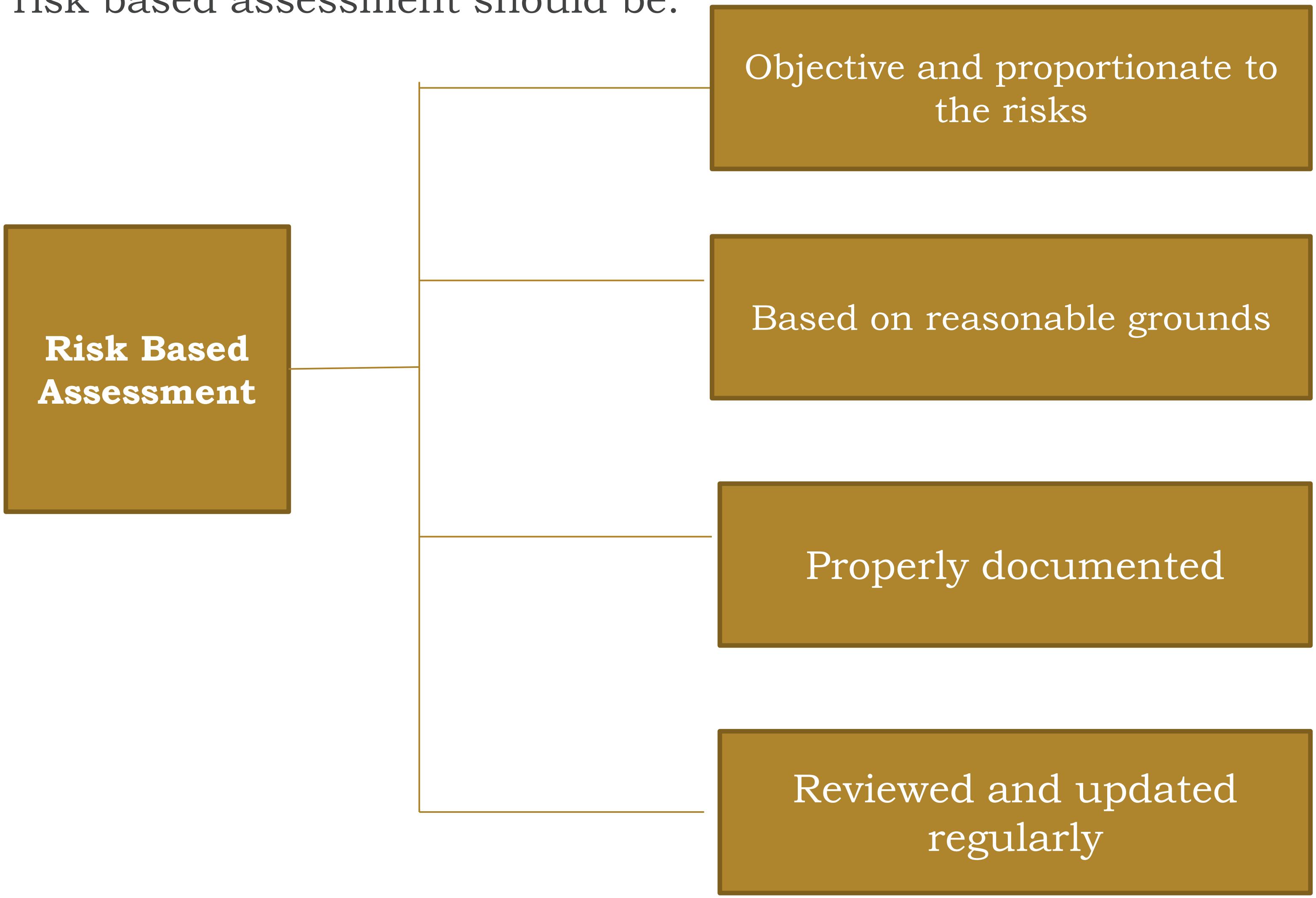
- RBA is an effective way to combat money laundering and terrorist financing.
- RBA:
  - ⇨ Recognizes that the ML/ TF threats vary across risk factors such as customers, countries, products and services, transactions and distribution channels.
  - ⇨ Allows an insurer to apply appropriate policies, procedures, systems and controls to manage and mitigate the ML / TF risks based on the nature, scale and complexity of the entity’s business and money laundering / terrorist financing risk profile.
  - ⇨ Facilitate effective allocation of resources to manage and mitigate the identified ML/ TF risks.

Risk Based Approach

- RBA determines the degree measures to be put in place to manage and mitigate the identified ML / TF risks:
  - ⇨ Low Risk – Simplified measures.
  - ⇨ Higher Risk – Enhanced measures.
- RBA should be incorporated into its existing policies and procedures as part of its overall risk management.

Risk Based Approach

- A risk based assessment should be:



Risk Based Assessment

Objective and proportionate to the risks

Based on reasonable grounds

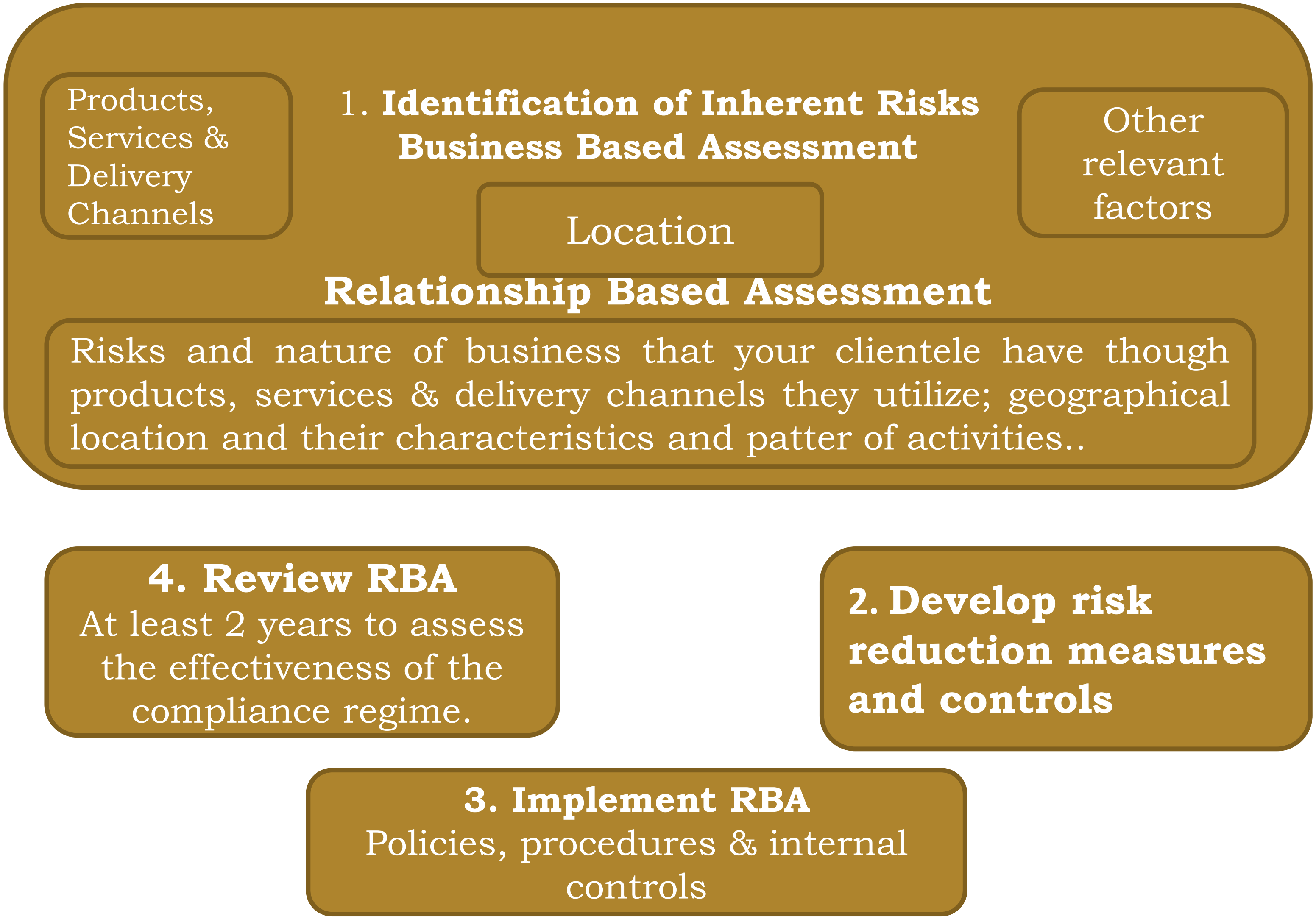
Properly documented

Reviewed and updated regularly

4

Risk-Based Approach Cycle

Risk-Based Approach Cycle



Products, Services & Delivery Channels

1. **Identification of Inherent Risks**

Business Based Assessment

Other relevant factors

Location

Relationship Based Assessment

Risks and nature of business that your clientele have though products, services & delivery channels they utilize; geographical location and their characteristics and patter of activities..

4. Review RBA
At least 2 years to assess the effectiveness of the compliance regime.

2. Develop risk reduction measures and controls

3. Implement RBA
Policies, procedures & internal controls

5

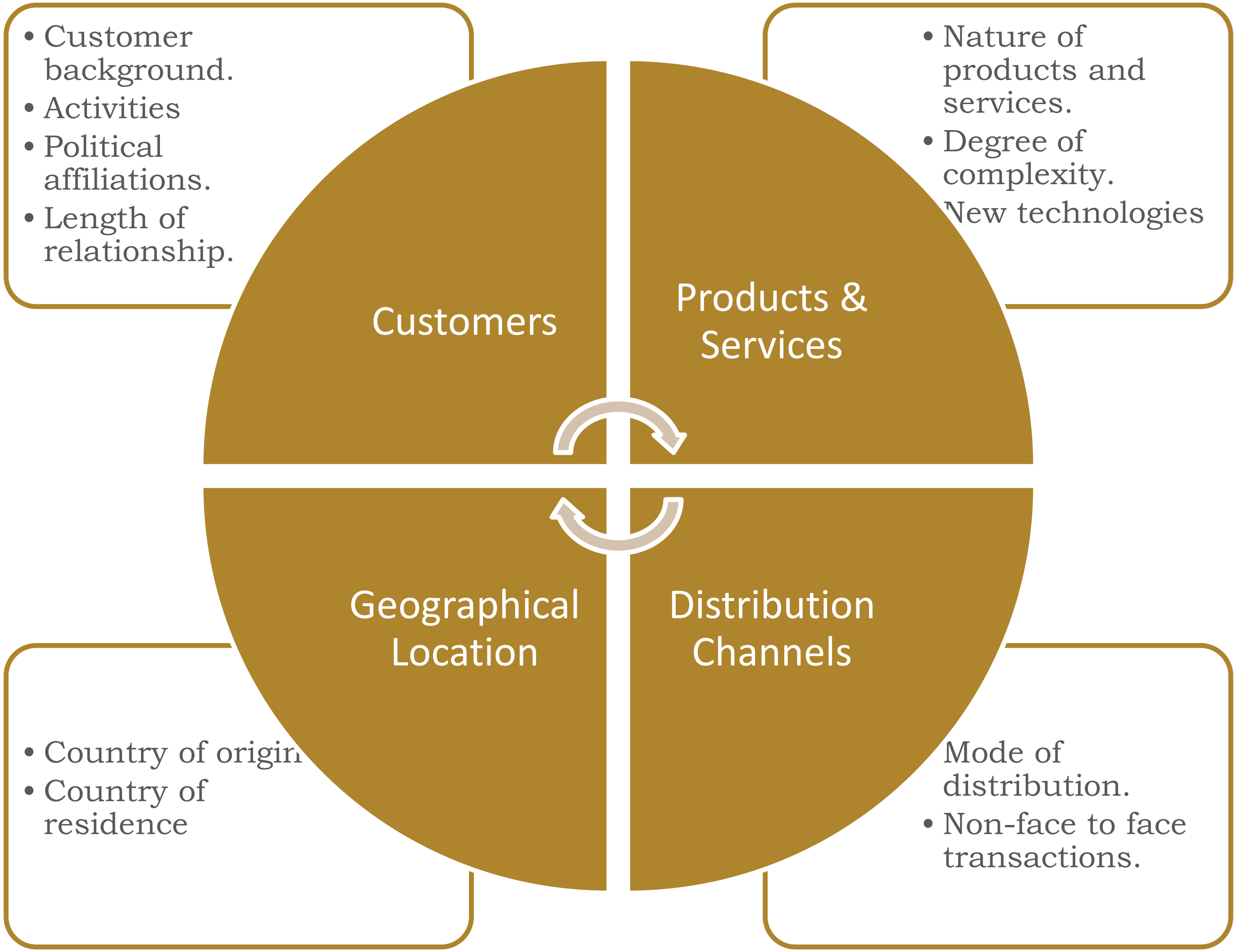
Identification of Inherent Risks

Identification of Inherent Risks

Insurance Regulatory Authority
Bima Bora kwa Taifa
IRA

- There is no standard methodology, can customize the following approach
- Should be done at two levels:
  - ⇨ Business-based risk assessment (BbRA) - identify and assess ML/TF risks associated with its business taking into consideration the nature, size and complexity of its activitiesand address the impact on its overall ML/TF risks.
  - ⇨ Relationship-based risk assessment (RbRA) – ML/TF risks associated with an insurer's relationship with its customers in terms of the types of products, services, distribution channels, geographical locations etc. that the customers are using and mitigate the risks identified.
- The outcomes of BbRA and RbRA complement each other.
- To effectively implement RBA:
  - ⇨ A regulated entity should determine reasonable risk factors and parameters for the BbRA and RbRA.
  - ⇨ Data from RbRA may be useful in updating the parameters of BbRA.

Risk Factors



Customers

- Customer background.
- Activities
- Political affiliations.
- Length of relationship.

Products & Services

- Nature of products and services.
- Degree of complexity.
- New technologies

Geographical Location

- Country of origin
- Country of residence

Distribution Channels

- Mode of distribution.
- Non-face to face transactions.

Business-Based Risk Assessment

- Identification of the inherent risks in an insurer’s business that makes it vulnerable to ML/TF.
- Assessment should take into account business-wide perspective so as to consider areas where risks could occur.
- Any area that is identified as high-risk requires documented mitigation strategies.
- An insurer should evaluate the likelihood and the extent of its ML/TF risks at a macro level and should consider all relevant risk factors, which include:
  - Products and services offered.
  - Transactions and distribution channels.
  - Geographical location.
  - Structure.
  - Findings of the National Risk Assessment (NRA).
  - Other specific risk factors that the regulated entity may consider for the purpose of identifying its ML/TF risks.

Business-Based Risk Assessment

- Assign a weight for each factor under consideration which individually or in combination may increase or decrease potential ML/TF risks posed to the regulated entity.
- Develop a risk scale tailored to the size and type of business.
- For example a simple low and high risk categories for small firms or more risk categories such as medium, medium-high or high for large firms.
- Any risk element that has been identified as "**high-risk**" must be addressed with mitigation measures and be documented.

Relationship-based Risk Assessment

Insurance
Regulatory
Authority
Bima Bora kwa Taifa
IRA

- Relationship-based risk assessment involves assessing the risk posed by the:
  - ⇨ combination of products, services and delivery channels the client uses;
  - ⇨ geographical location of the client and of their transactions; and
  - ⇨ client's characteristics, patterns of transactions, etc.
- Some of the indicators that automatically place clients in the high-risk category include:
  - ⇨ politically Exposed Person (PEP);
  - ⇨ legal entity with a complex structure that conceals the identity of beneficial owners;
  - ⇨ possibility that the client is in possession or control of property that is believed to be owned or controlled by or on behalf of a terrorist or a terrorist group;
  - ⇨ cash-intensive business;
  - ⇨ a suspicious Transaction Report (STR) was previously filed or considered; and
  - ⇨ account activity does not match the client profile.

Relationship-based Risk Assessment

Insurance Regulatory Authority
Bima Bora kwa Taifa
IRA

- An insurer should put in place enhanced measures for a client or groups of clients that have been identified as high risk.
- The measures should be documented.
- Identifying one high-risk indicator for a client does not necessarily mean that there is a high-risk client relationship.
- A relationship-based risk assessment model ultimately **draws together** the products, services and delivery channels used by your client; your client's geographical risk; and your client's characteristics and patterns of activities.
- An insurer may consider using a likelihood and impact matrix when scoring relationship-based risk assessment so as to determine the level of effort or monitoring required for the identified inherent risks.
  - ⇨ **Likelihood** - The chance of the risk being present.
  - ⇨ **Impact** - the consequences of the damage if the assessed risk materialized.

6

Risk Reduction Measures

Risk Reduction Measures

- Develop and implement controls to limit the identified ML/TF risks.
- The controls should be commensurate to the identified risks.
- An ML/TF risk that has been assessed as high requires documented risk mitigation strategies – policies and procedures.
- Should put in place internal controls that will help in mitigating the overall risk.
- All high-risk elements that have been identified as part of the **business-based risk assessment** have to be mitigated by controls which should be documented.
- With respect to relationship-based risk assessment, an insurer will have to conduct ongoing monitoring and keep a record of the measures and information obtained.
- High-risk clients and business relationships require more frequent monitoring and enhanced measures to ascertain the identification and/or keep client information up to date.

7

Implement Risk-Based Approach

Implement Risk-Based Approach

Insurance Regulatory Authority
Bima Bora kwa Taifa
IRA

- Implement the RBA as part of its day-to-day activities and any existing obligations, such as client identification, should to be maintained as a minimum baseline requirement.

- The risk assessment should be documented as part of the compliance regime.

- Compliance policies and procedures should be communicated, understood and adhered to by all the staff dealing with clients.

8

Review Risk-Based Approach

Review RBA

- An insurer should conduct a periodic review (minimum every 2 years) of its risk assessment to test the effectiveness of the compliance regime.
- The following should be reviewed:
  - ⇨ Policies and procedures;
  - ⇨ Risk assessment related to ML/TF; and
  - ⇨ Training program (for employees and senior management).
- In addition, the risk assessment should be updated along with the policies and procedures, mitigating measures and controls any time the business model changes or when new products and services are introduced.

9

Purpose of a Risk Assessment

Purpose of a Risk Assessment

Insurance Regulatory Authority
Bima Bora kwa Taifa
IRA

- The results of a risk assessment can be used for a variety of reasons, including to:
  - ⇨ identify gaps or opportunities for improvement in AML policies, procedures and processes;
  - ⇨ make informed decisions regarding implementation of control efforts, allocation of resources, technology spend;
  - ⇨ decide whether or not to continue a high risk product;
  - ⇨ set limits to restrict exposure to certain customer types/ products/ regions;
  - ⇨ understand how the structure of a business unit or business line’s AML compliance programme aligns with its risk profile;
  - ⇨ develop risk mitigation strategies including applicable internal controls to reduce a business unit or business line’s residual risk exposure;
  - ⇨ ensure senior management and board are aware of the key risks, control gaps and remediation efforts; and
  - ⇨ Ensure that regulators and other authorities are made aware of the key risks, control gaps and remediation efforts across the entity.

10

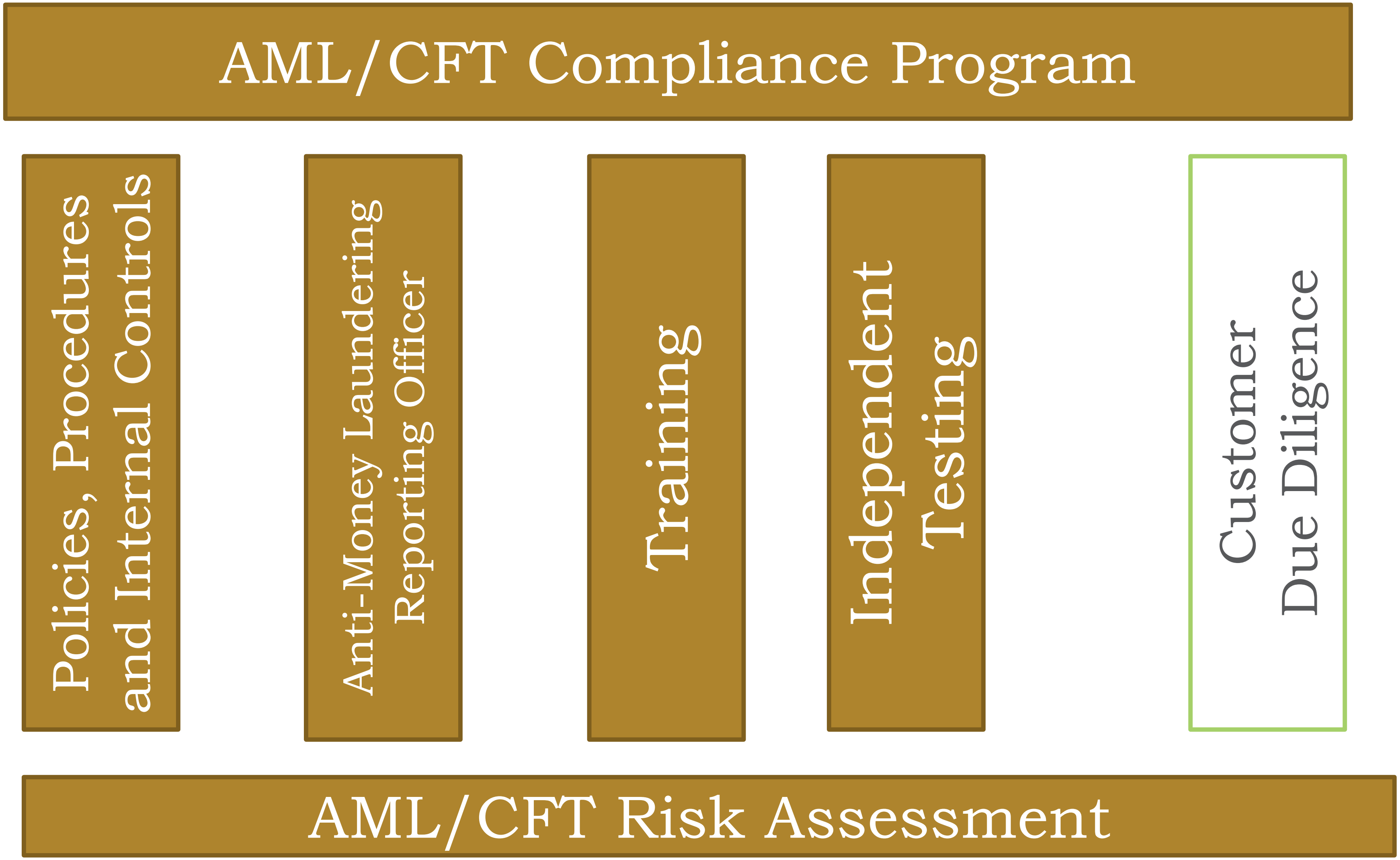
Compliance Program

Compliance Program

- AML/ CTF compliance programmes should ideally be risk based, not transaction driven or purely rules based.
- The process begins with an assessment of the ML and TF risks that an insurer is exposed.
- The results are then used to develop effective measures to monitor and mitigate the risk.

Compliance Program

- An effective AML/CFT compliance program consists of:



AML/CFT Compliance Program

Policies, Procedures and Internal Controls

Anti-Money Laundering Reporting Officer

Training

Independent Testing

Customer Due Diligence

AML/CFT Risk Assessment

Compliance Policies and Procedures

- At a minimum, the compliance policies and procedures should incorporate:
  - ⇨ Reporting;
  - ⇨ Recordkeeping;
  - ⇨ client identification;
  - ⇨ risk assessment; and
  - ⇨ enhanced measures for high risks.
- Policies and procedures should:
  - ⇨ Document the process of detecting suspicious transactions and dealing with such situations;
  - ⇨ Determine and explain what kind of monitoring is done for particular situations (i.e. low vs. high-risk clients / business relationships);
  - ⇨ Describe all aspects of your monitoring:
    - – when it is done (its frequency),
    - – how it is conducted, and
    - – how it is reviewed.

Thank You!