Public and Private Sector Surveys Report on Financial Integrity and Financial Inclusion Frameworks and Compliance Practices

Alliance for Financial Inclusion / Eastern and Southern Africa Anti-Money Laundering Group

September 2013

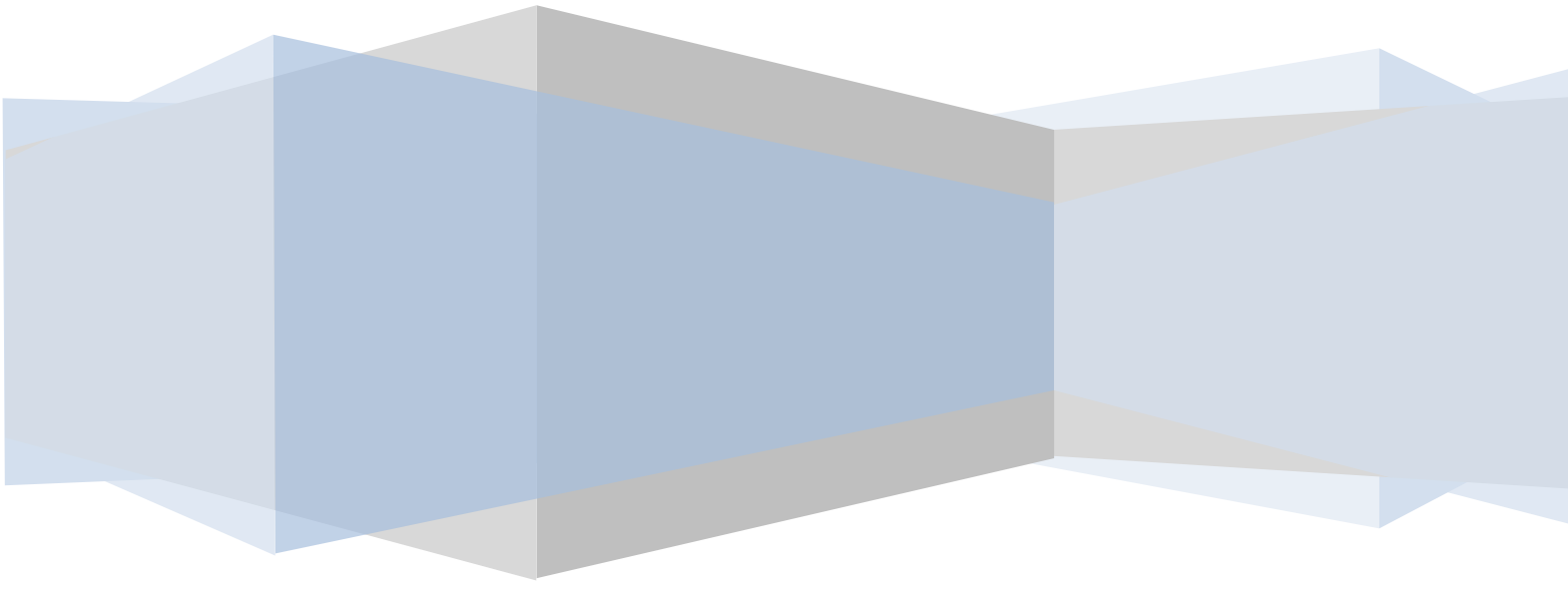

Table of contents

1 INTRODUCTION

The Ad-hoc Working Group on Financial Inclusion (the Working Group) of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), with the support of the Alliance for Financial Inclusion (AFI), undertook two surveys in the third and fourth quarters of 2012:

- A public sector inventory of Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF) policies, frameworks and attitudes relevant to financial inclusion; and
- A private sector survey of money laundering (ML) and terrorist financing (TF) risk assessment and risk mitigation practices relating to the low-income sector.

The main objective of the surveys was to identify the key areas where the Working Group on Financial Inclusion can make a useful contribution to the development of policy, law and practices to align financial inclusion and financial integrity in the ESAAMLG region. The public sector survey was undertaken to gauge the level of current policies, laws and attitudes relating to financial integrity and financial inclusion amongst the members of the Working Group. The public sector survey was completed by Malawi, Mozambique, Namibia, South Africa, Uganda, Zambia and Zimbabwe.

The private sector survey probed current compliance practices and challenges to identify the need for and contents of a potential engagement by the Working Group with the private sector. In total, 83 responses were received from institutions in 12 countries:

Country	**Private sector reports**
Botswana (co-chair)	11
Comoros	1
Kenya	11
Lesotho	4
Malawi	14
Mauritius	19
Mozambique	2
Namibia Co-chair	1 (joint industry report)
South Africa	6
Swaziland	1
Zambia	7

Zimbabwe	6
	83

An interim report on the private sector survey was prepared on 15 January 2013. This report was discussed by the Working Group at their meeting in Arusha, Tanzania, on 10 April 2013. The Working Group agreed that the report should be enhanced with an analysis of the public sector responses and that a consolidated report with recommendations for action should be prepared for the Working Group.

1.1 STRUCTURE OF THE REPORT AND ANALYSIS OF SURVEYS

The report is structured into three distinct sections:

- Section 2 discusses the findings of the public sector survey;
- Section 3 discusses the private sector responses; and
- Section 4 closes with recommendations for further action.

The analysis of the public and private sector surveys is limited in this report. While the respondents provided very useful perspectives to further the internal discussions and the engagement project of the Working Group with the private sector, the responses do not lend themselves to comparative or quantitative analysis. The private sector respondents range from large, international institutions to very small service providers, often with very different products and with very different challenges given differences in the national context. A comparative analysis of the responses is therefore not useful. While the private sector reports filed by large banks were often more comprehensive than those filed by smaller institutions, many responses were incomplete. Further engagement with each respondent will be required to gain accurate and comprehensive information.

The data and comments in relation to a number of questions are however very useful to identify further work that could be undertaken by the Working Group. They are indicative of trends that should be noted and ranges of practices that are currently employed in the region. The report therefore highlights these trends and the ranges of practices but focuses on suggested actions that the Working Group can take.

Please note that this report reflects policies, laws and AML/CFT frameworks as in November 2012.

1.2 SUMMARY OF RECOMMENDATIONS

Three broad sets of Recommendations are made:

- Recommendations for similar studies in the future;
- Recommendations for engaging with ESAAMLG members; and

- Recommendations for engaging with the private sector.

These Recommendations are outlined in greater detail in Section 4.

1.2.1 Recommendations for similar studies in the future

The design of similar studies in future should ideally involve either on-site visits to the relevant parties or national workshops where participants can share and debate their views, informing a consolidated national report that is submitted to ESAAMLG.

1.2.2. Recommendations for engaging with ESAAMLG members

1.2.2.1 Supporting the development of national policy and legal frameworks

The Working Group should organise a peer learning workshop for ESAAMLG members to support the drafting of comprehensive national policy and legal frameworks that would balance financial integrity and financial inclusion policy objectives. Such policies should ideally

- Align the financial inclusion and financial integrity objectives and programmes of action of the government departments, agencies and regulators involved in different aspects of financial integrity and financial inclusion;

- Enable the development of legal and regulatory frameworks that permit risk-based implementation of the FATF standards, especiallyfor appropriate new payments systems and new service delivery channels;

- Empower regulators to assess money laundering and terrorist financing risks of new payments systems and new service delivery channels and advise appropriate controls that balance financial inclusion and financial integrity objectives; and

- Respond appropriately to national opportunities and address the objectives and challenges of service providers and vulnerable users.

1.2.2.2 Simplified CDD for cross-border transactions and services

The Working Group should

(1) Investigate whether there is a need for appropriate simplified CDD in relation to cross-border financial transactions amongst ESAAMLG member countries; and, if so,

(2) Advise the Ministerial Council on the most appropriate ways to ensure that appropriate proportional controls are imposed where risk is lower.

1.2.2.3 Risk assessments

The Ministerial Council should ask each member of ESAAMLG to file a report with ESAAMLG within six (6) months of completing its initial risk assessment, sharing its risk assessment methodology, the challenges it encountered when undertaking the assessment, and proposals to improve its data and processes in future.

1.2.3 Recommendations for engaging with the private sector

Each Working Group member should review the private sector reports submitted by the institutions of their countries and engage the respondents, as well as other stakeholders, to determine which of the matters identified in Section 4.3 of the report should be addressed nationally and which should be addressed regionally, and report their findings to the Working Group;

If appropriate topics for regional guidance are identified, the Working Group should engage private sector representatives at a regional workshop to:

a) Map potential guidance in relation to the identified matters;
b) Design processes, potentially by working in multi-disciplinary working groups, to produce draft guidance relating to appropriate practices, and
c) Submit draft guidance to the Ministerial Council of the ESAAMLG for approval.

2 PUBLIC SECTOR INVENTORY OF AML/CFT POLICIES, FRAMEWORKS AND ATTITUDES RELEVANT TO FINANCIAL INCLUSION

2.1 NATIONAL POLICY AND LEGAL FRAMEWORK

The first set of questions of the public survey questionnaire addressed the national policy framework and legal framework for financial integrity and financial inclusion. The findings are summarised in **Box 1**.[1]

1 The comments made by countries and reflected in the series of text boxes were subject to minimal editing to ensure consistency and clarity. The ESAAMLG Secretariat has copies of the original submissions.

Box 1

Country	AML /CFT laws	National identifi-cation frame-work	Formal policy on financial inclusion[2]	Policy frame-work for mobile money	Policy frame-work for prepaid cards	May financial services be rendered through agents?	Under-taken national ML/FT risk assess-ment
Malawi	Yes	No	Yes[3]	Yes	Yes	No[4]	In process
Mozambique	Yes	Yes	Yes	No	No	No	No
Namibia	Yes	Yes	In develop-ment	Yes	No	No	In process
South Africa	Yes	Yes	In develop-ment	In develop-ment	In develop-ment	Yes	In process
Uganda	In part[5]	No	No[6]	In develop-ment[7]	No	No	No
Zambia	Yes	Yes	In develop-ment	In develop-ment	In develop-ment	Yes	Planned for 2013-2018

2 Many countries that participated in the survey have regulatory measures that promote financial inclusion or allow mobile money services to be rendered or prepaid cards to be issued. This question focused on whether they have a comprehensive and formal policy framework that supports their financial inclusion measures.

3 Malawi National Strategy for Financial Inclusion (2010-2014).

4 Section 24(6) of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act 11 of 2006 allows CDD to be undertaken by third parties and intermediaries.

5 Uganda's Anti-Terrorism Act of 2002 criminalises terrorist financing. AML/CFT compliance by financial institutions is regulated and supervised in terms of the Financial Institutions (Anti-Money Laundering Regulations), 2010. Uganda did not have an Act criminalising money laundering when the survey was completed, but envisaged adopting a money laundering law in 2013.

6 Financial inclusion is being addressed as a comprehensive project at the Bank of Uganda.

7 Mobile services are allowed by means of "no objection" letters issued by the Bank of Uganda.

Zimbabwe	Yes	Yes	Yes[8]	No	No	Yes	No

The findings reflect a region where both financial inclusion and financial integrity are important policy objectives. Most countries surveyed have adopted AML/CFT laws and are developing policy and regulatory frameworks regarding financial inclusion. The region is grappling with the implementation of the 2012 revised FATF Recommendations and especially the new mandatory risk-based approach (RBA) to AML/CFT. At the date of completion of the surveys, none of the countries had yet completed its risk assessment. Malawi, Namibia and South Africa were, however, in the process of undertaking a national risk assessment as part of their RBA, while the other countries were planning or considering such an assessment.

Financial inclusion initiatives were supported in all the countries that participated in the survey. The financial inclusion policy frameworks of the countries were, however, at different stages. Most countries had some policy elements in place but few countries had formal and comprehensive policy frameworks on financial inclusion. Many countries had some elements of policy relating to mobile money, prepaid cards and agent banking and financial services.

The fact that countries share the same financial integrity and financial inclusion objectives but are at different stages of the development of their policies and processes provides an opportunity for a peer-learning programme where members can share experiences and learn from each other. Each country has its own unique context and faces its own challenges. Not all countries in the region, for example, have national identification frameworks. Out of the seven countries, five have national identification frameworks. There is, however, a sufficient depth of shared contexts and challenges to ensure a rich and meaningful exchange.

8 Although Zimbabwe does not have formal financial inclusion policy, it has a legal framework to prohibit the use of cash for certain transactions and to compel and promote the use by the public of financial institutions for the purpose of mediating, facilitating or obviating cash transactions. The promotion measures are linked to its AML/CFT measures and are enforced the Bank Use Promotion and Suppression of Money Laundering Unit (currently known as the Financial Intelligence Evaluation and Security Unit. This Unit, which is within the Reserve Bank of Zimbabwe, was established by the Bank Use Promotion and Suppression of Money Laundering Act [Chapter 24:24] Acts 2 of 2004 and 16 of 2004.

2.2 LOW-RISK INSTITUTIONS, PRODUCTS, CLIENTS AND SERVICES

The second part of the questionnaire, explored the extent to which ESAAMLG members utilised the flexibility allowed by the FATF Standards to support financial inclusion (see **Box 2**).

Although the governments concerned give a high priority to financial inclusion and to financial integrity, much work still remains to improve the alignment between these two policy objectives. The legal framework of the country must for example allow simplified CDD. Only four of the seven countries allow their institutions to undertake simplified Customer Due Diligence (CDD) measures (see **Box 2**). None of the countries, however, allow simplified CDD measures in relation to cross-border financial services.

Furthermore, in terms of the FATF Standards decisions to subject specific clients, products or services to simplified CDD, must be informed by appropriate risk assessments. While some of the countries that were surveyed have made good progress with their national risk assessments, no country reported that it had completed its assessment (see **Box 1**). While a number of countries advised their financial institutions to undertake institutional risk assessments, only two countries (Zambia and Zimbabwe) reported that their institutions were compelled to do so (see **Box 2**). Only two countries (Namibia and South Africa) indicated that they exempted some financial institutions from AML/CFT duties because they pose a low risk.

Box 2

Country	Are any financial institutions exempted from AML/CFT duties because they pose a low risk?	Are institutions compelled to undertake ML/FT risk assessments of clients, products and services[9]	Is simplified CDD allowed?	Is simplified CDD allowed for cross-border financial services?
Malawi	No	In development	Yes	No
Mozambique	No	No	No	No
Namibia	Yes	No	No	No

9 Countries generally indicated that institutions are not compelled to undertake a risk assessment, but that regulators encourage them to do so.

South Africa	Yes	No	Yes	No
Uganda	No	No	No	No
Zambia	No	Yes	Yes	No
Zimbabwe	No	Yes	Yes	No

2.2 VIEWS HELD BY NATIONAL POLICYMAKERS AND REGULATORS

The third part of the questionnaire investigated various views held by the policymakers and regulators.

2.2.1 Meaning of "low risk"

Question 16 asked participants to share their views relating to the meaning of "**low risk".** What does it mean if a product, service or client is classified as posing a low risk for money laundering or terrorist financing purposes? What are the risks that they would consider relevant and what do they understand by "low"?

The FATF's RBA standards distinguish between "low" risk and "lower" risk[10]. The exemption of institutions from AML/CFT obligations may be considered by a country in very specific, limited and proven low-risk cases but the recommendations allow countries to consider allowing the application of simplified CDD measures where risks are lower. FATF does not define these concepts, nor does it determine when a risk can be classified as the one rather than the other.

The country responses (see **Box 3**) reflect a large measure of consensus. In general, ML/FT risk is viewed as low when the probability of abuse of a product or service, or the probability of involvement of a client in ML/FT, is low and where the impact is also low, should it occur. Malawi raises an important point relating to a difference in the levels of ML and FT risk in terms of this approach: In respect of the same transaction and the same amount, FT risk rating would tend to be higher than the ML risk rating as the impact of terrorist financing would tend to be higher when it occurs.

Factors that countries consider as pointing towards a low-risk level for products and services include:

10 See FATF *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion* (2013) parr 37 and 69.

- A lack of cross-border functionality or no transaction involving high-risk jurisdictions;[11]
- Products with basic functionality;
- Very low transactional values; and
- Tried-and-tested products with embedded transaction limits and a good audit trail.

The respondents describe a low-risk client as one who is unlikely to engage in criminal activities and unlikely to be introducing proceeds of crime into the financial system. Relevant factors to consider include their line of business, the size and frequency of transactions, geographical location, etc. Potential examples of low-risk clients include:

- Salaried employees of reputable organisations;
- Earners of very low and predicable monthly/weekly income; and
- Clients who are not making funds transfers to high-risk jurisdictions, areas or organisations.

	Box 3
Country	**What does it mean if a product, service or client is classified as posing a low risk for money laundering or terrorist financing purposes? What are the risks that you consider and what do you understand under "low"?**
Malawi	(1) It means that the probability of that particular product, service or client being used for ML/FT purposes is low. And the impact would also be low. But of course, this would be tricky for FT - the impact is always big. (2) Secondly, it means that a financial institution can use simplified CDD in relation to such a product, customer or service. Elements indicating lower risk: low value; basic products; locally accessed; no involvement of third parties
Mozambique	Low, medium or higher risk can be measured according of the vulnerability of product, service or client to facilitate ML/FT activities
Namibia	Overall, a product that based on it features is unlikely to be used in a ML/FT Features such as no cross border transactions or extremely low values. Similarly low risk clients will be those that have a very low probability of introducing proceeds of crime in to the financial system due various factors which, if present, lowers the risk. Factors such as being a salaried employee at a reputable organisation or when earning a very low and predicable monthly/weekly income and not making funds transfers to high-risk jurisdictions or areas or organisations would substantiate an assessment of

11 Uganda and Namibia would also allow low value cross-border transactions between countries with sound AML/CFT regimes to be classified as low risk.

	low risk assigned to a customer.
South Africa	It means that there is a low likelihood of the product or service in question being used as a mechanism to launder the proceeds of crime or to provide financial support for terrorist organisations or activities, or if this were to happen the impact would be negligible.
Uganda	Low risk would apply to a customer, service or product that is unlikely to result money laundering. Examples might include: an unsophisticated client who is unable to "hide" their actions; low-cash transactions with visible lawful purpose; low-value transactions between countries with strong AML/CFT regimes; tried-and-tested products with embedded transaction limits, good audit trail; cash-in / cash-out money transfers on a real-time basis, and strong internal controls, among others.
Zambia	Infrequent transactions involving insignificant value.
Zimbabwe	In respect of a product or a service, it simply means that the product or service is one that is unlikely to attract the interest of criminals or, where it does, not much harm is likely to result from use by criminals. In respect of persons, low risk means the person is deemed to be unlikely to engage in criminal activities, given their line of business, size and frequency of transactions, geographical location, etc.

2.2.2 Low-value transactions

The questionnaire probed what respondents would rate as a low-value transaction in their jurisdiction, notably a transaction that would pose a low risk because it involves limited value?

One respondent indicated USD 100, another indicated USD 200, four indicated USD 500 and one indicated USD 1000. Respondents indicated that their answers and views were informed by factors in their economy and the general income levels of clients as well as existing controls. See **Box 4** below.

While the differences were expected and countries are correctly considering their own national contexts when determining appropriate low value amounts, the differences will need to be considered when low-risk parameters are designed for cross-border financial services such as remittances (see par 4.2.2. below).

Two respondents indicated in their responses that risk is not determined by the amount alone and that other factors such as the client profile should also be considered. This view is also expressed more generally in par 2.5 and **Box 7** below.

Box 4		
What would you rate as a low value transaction in your jurisdiction, i.e. one that would pose a low risk because it involves limited value?		
Malawi	Less than USD 200	Transactions below USD 200 as most Malawians would earn this much legally (for example government salaried employee and peasant farmers).
Mozambique	Less than USD 100	The medium minimum wage is around USD 100.
Namibia	Less than USD 500	USD 500 or the equivalent of N$5,000 would be considered a low-value amount. Please note that a low-value transaction would not always translate into a low-risk transaction. The amount should be considered together with the client profile and the person's transactional history and behaviour.
South Africa	Less than USD 500	
Uganda	Less than USD 500	The local currency transaction limits for ATMs and mobile money transfers approximates to this amount. For foreign exchange transactions, amounts below USD 10,000 are considered low risk. Note that not only the amount but also the nature of the transaction and the behaviour of the customer determine the risk level.
Zambia	Less than USD 1000	This is the limit currently being used for money or value transfer services without requiring enhanced CDD.
Zimbabwe	Less than USD 500	This is based on a value judgment taking into account the size of the country's economy.

2.2.3 Capacity of financial institutions to implement RBA

The questionnaire asked about capacity of countries' institutions to implement a RBA in relation to AML/CFT. Countries were asked to respond to the following statement: "*The capacity and understanding of many financial institutions in my jurisdiction are too limited to undertake appropriate risk assessment and design appropriate controls.*"

Two countries agreed with the statement but the majority disagreed (see **Box 5**). It seems as if the majority of the respondents focused on the capacity of large financial institutions. In many cases smaller banks and, as Zimbabwe pointed out, non-bank financial service providers may have more limited capacity to implement an RBA. This is borne out by the responses received from the private sector. The private sector responses (see Section 3 below) indicate that smaller institutions have significant capacity challenges relating to AML/CFT, risk assessment and risk mitigation.

Capacity to implement and manage an AML/CFT RBA is a matter that the Working Group should explore for potential private sector engagement at a national or regional level (see par 4.3 below). The Working Group may be able to assist national regulators to increase such capacity in relation to low and lower risk products, services and clients.

Box 5

The capacity and understanding of many financial institutions in my jurisdiction are too limited to undertake appropriate risk assessment and design appropriate controls.		
Malawi	Agree	Many financial institutions in Malawi do not undertake appropriate ML/FT risk assessments because they do not understand how to conduct them. Non-bank financial institutions have less experience in implementing AML/CFT measures and their understanding and capacity are probably lower than that of banks. Having noticed this gap we have drafted the ML Guidance Note.
Mozambique	Disagree	We do not agree since financial institutions have risk policies that include risk assessment. In addition, the majority of banks operating in Mozambique have a parent company outside the country.
Namibia	Agree	Lacking a proper understanding of the importance and value of identifying, assessing and treating inherent ML/FT risks, financial institutions currently are reluctant to perform these risk assessments. A proposed amendment to the FIA now making it mandatory. Secondly, AML/CFT expertise is very scarce and guidance on how to conduct appropriate risk assessments is even scarcer.
South Africa	Disagree	South African financial institutions are well capacitated with skilled and experienced professional who are more than capable of undertaking appropriate risk assessment and designing appropriate controls.

Uganda	Disagree	Financial institutions are required to have documented policies to guide their AML controls. Staff members are also trained to identify/recognise and report ML/FT issues.
Zambia	Disagree	Financial service providers are required under prudential regulation (RBA) to profile their risks and they have done that in the past.
Zimbabwe	Disagree	Financial institutions in Zimbabwe, especially banks, are relatively well-informed in AML/CFT measures, which they have been implementing for a very long time now, and are capable of carrying out proper risk assessments and to design appropriate controls. Non-bank financial institutions, however, have less experience with implementing AML/CFT measures and their understanding and capacity is probably lower than that of banks.

2.2.4 Proceeds of crime, formal financial services and the informal economy

When simplifying CDD measures in a financial inclusion context, regulators often have to balance financial exclusion risk (i.e. the risk associated with cash and cash proceeds of crime that remain outside the formal financial system in the informal economy) with financial inclusion risks (that simplified controls may allow small amounts of proceeds of crime to enter the formal financial sector). To investigate the views of countries, the questionnaire requested countries to respond to the following statement: "*It is better to keep proceeds of crime in cash in the informal economy than to allow it to slip into the formal financial sector as a result of weak AML/CFT controls.*"

Respondents interpreted the question in different ways. In general, respondents were concerned about protecting the integrity of formal financial services but also about the abuse of the informal sector. Respondents pointed out that continuing abuse of the informal sector would have the following consequences:

- Prevent detection and punishment of criminals because it is more difficult to follow money trails in the informal sector;
- Allow criminals to benefit from proceeds of crime, providing an incentive for criminals to continue with profit generating crime;
- Enable criminals to accumulate financial power that can be abused for further criminal purposes such as corruption;
- Prevent detection and punishment of criminals;
- Distort tracking of monetary aggregates; and
- Potentially create asset-price bubbles and push up prices.

See **Box 6** for the comprehensive responses.

		Box 6
It is better to keep proceeds of crime in cash in the informal economy than to allow it to slip into the formal financial sector as a result of weak AML/CFT controls.		
Malawi	Agree	If we allow proceeds of crime in cash to slip into the formal financial sector as a result of weak AML/CFT controls, we would encourage money launderers to continue the act. If this can be prevented from entering the financial system, there will be no motivation for the act.
Mozambique	Agree	If criminals realize that a country's AML/CFT is weak and the regulator allows the cash proceeds of crime to slip into the formal sector, it suggests that that policy may facilitate the launders to invest that money in other activities and create a multiplier effects. But if the criminals remain in the informal sector, they will not have a market to invest that proceeds.
Namibia	Disagree	Governments all over the world need to realise that money spent establishing robust compliance regimes should not be considered an expense, but a recoverable investment. If the funds are left in the informal economy, the probability to recover taxes or even any portion of the proceeds of crime is very low. Balancing financial inclusion efforts with integrity is essential as any form of ML/FT occurring, for example through the informal economy, would be unstoppable and probably untraceable. In conducting a national ML/FT risk assessment it is imperative that the ML/FT risk associated with the size of the informal economy is identified and evaluated as this could be a real threat to the overall effectiveness and objectives of the national AML/CFT regime.
South Africa	Disagree	There should be no room for weak AML/CFT controls in order to preserve the safety and soundness of the country's financial sector and to ensure that proceeds of crime are not used to perpetuate criminal activity. Restricting the cash proceeds of crime to the informal economy still allows criminals to benefit from proceeds of crime, providing an incentive for criminals to continue with profiting from crime. It also allows criminals to accumulate financial power that can be abused for further criminal purposes such as corruption.
Uganda	Disagree	Keeping proceeds of crime in the informal sector prevents detection and punishment of the culprits, distorts tracking of monetary aggregates and can create asset-price bubbles and push

		up prices.
Zambia	Disagree	It should never be appropriate (and it is illegal in Zambia) to keep proceeds of crime once identified as such. In any case, financial inclusion enhances the chances of developing customer profiles and therefore allows the application of the legal and regulatory oversight for purposes of AML/CFT.
Zimbabwe	Agree	The main purpose of AML/CFT controls, including CDD measures, is to keep proceeds of crime out of the formal financial system. There is merit in maintaining the integrity of the financial system by preventing its misuse by criminals. The downside of such policies is that laundering can still occur outside the formal financial system through cash transactions and it is often harder to investigate ML/FT offences committed outside the formal financial system as there is often little paper trail to go by. That said, maintaining the integrity of financial institutions overrides the facility of financial investigations offered by a formal paper trail.

2.2.5 Focus on larger or smaller transactions

Respondents were asked whether countries should focus their AML/CFT systems on larger transactions. They were asked to respond to the following statements: "*No AML/CFT framework can prevent all criminal transactions. The framework should therefore focus on larger transactions and allow small transactions to be concluded anonymously*."

Generally, countries that expressed a view on the first statement agreed that AML/CFT frameworks cannot prevent all criminal transactions. Countries generally agreed that the RBA required a focus on higher-risk transactions, but pointed out that value is not the only indicator of risk. If attention was only given to larger transactions, criminals may abuse smaller transactions to split their proceeds of crime and launder it through a series of smaller transactions. While the FATF Standards do not compel institutions to undertake CDD on small, one-off transactions, none of the respondents were prepared to endorse small, anonymous transactions. Zambia responded that all clients must be identified irrespective of the value of the transaction, but that the extent of verification of identities could vary with the level of risk posed by the transaction. See **Box 7** below.

Box 7
No AML/CFT framework can prevent all criminal transactions. The framework should therefore focus on larger transactions and allow small transactions to be concluded anonymously.

Malawi	Agree	Efforts to prevent criminal transactions should be focussed on large transactions because they have a significant impact on the economy, especially as we are encouraging risk-based assessment.
Mozambique	Disagree	Although money launders generally use high-value transactions, they may start making a lot of low-value transactions anonymously if they realise that banks are more concerned about high-value transactions.
Namibia	Agree	Considering the law of large numbers, it is highly unlikely.
South Africa	Disagree	The size and value of transactions are not the only indicators of ML/FT risk. Focus should not only be on larger transactions but on any suspicious transactions, regardless of the value of the transaction, as criminal elements could utilise a series of small transactions to disguise criminal proceeds or the movement of funds destined to support terrorist organisations or activities.
Uganda	Disagree	ML/FT transactions can be broken down into small transactions to prevent detection. The framework should therefore concentrate on the nature and risk profiling of person involved in order to detect unusual transactions.
Zambia	Disagree	The AML/CFT framework allows for transparency of transactions in an economy. As such, customers involved in all transactions regardless of size need to be identified. It is the extent of verification of identities that should vary with the level of risk posed by the transaction.
Zimbabwe	Disagree	It is correct that no AML/CFT framework can prevent all criminal transactions. It is, however, erroneous to focus on larger transactions and ignore small transactions. AML/CFT risk is not necessarily correlated to the size of the transaction. The transactions on which to focus should be identified by a proper risk assessment of the transaction and the customer.

2.2.6 Enhanced monitoring

The respondents replied unanimously that they agreed with the following statement: "*ML/FT risk introduced by simplified identification and verification measures can be mitigated by enhanced monitoring of transactions, if designed properly.*"

Two caveats were listed (see **Box 8** below):

- Electronic monitoring systems can be very expensive, and limited guidance is available to calibrate the systems correctly; and
- Enhanced monitoring of completely anonymous transactions is of little value.

Box 8		
ML/FT risk introduced by simplified identification and verification measures can be mitigated by enhanced monitoring of transactions, if designed properly.		
Malawi	Agree	Financial institutions in Malawi are encouraged to have systems in place that will monitor transactions of clients who have been identified by simplified measures so they can enhance CDD when transactions are above the threshold.
Mozambique	Agree	Despite the implementation of simplified CDD, monitoring of transaction is always necessary because this group of low-risk customers may be used by launderers.
Namibia	Agree	If there is a clear understanding of the ML/FT associated risks with the monitoring controls, then the risks would be adequately mitigated. These monitoring controls cost a lot of money however with not a lot of guidance or expertise being available to design these controls accurately.
South Africa	Agree	Enhancing monitoring controls combined with appropriate levels of CDD would ensure the identification of suspicious transactions for both high- and low-risk financial products. Enhanced monitoring of completely anonymous transactions is of little value for mitigating the risk of money laundering or terrorist financing.
Uganda	Agree	Monitoring helps to validate the risk assessment and detect early on previously unenvisaged risk.
Zambia	Agree	Enhanced monitoring allows for better understanding of the

		changing risk profiles of customers on an on-going basis.
Zimbabwe	Agree	Simplified identification and verification measures introduce some ML/FT risk. It is therefore essential that whenever such measures are implemented, enhanced monitoring of transactions occur.

3 PRIVATE SECTOR SURVEY OF AML/CFT CONTROLS RELEVANT TO FINANCIAL INCLUSION

As pointed out in the Introduction, the responses provided by the private sector respondents do not lend themselves to comparative or quantitative analysis.

The respondents range from large, international financial institutions to very small financial service providers, often with very different products and with very different challenges given differences in the national context. A comparative analysis of the responses is therefore not useful. The private sector reports filed by large banks were often more comprehensive than those filed by smaller institutions, many responses were incomplete. Further engagement with each respondent will be required to gain accurate and comprehensive information.

While surveys do not lend themselves to a comprehensive comparative quantitative or qualitative analysis, the responses do provide very useful perspectives on broad trends. These are valuable for informing internal discussions and how the Working Group engages with the private sector.

This section provides a general overview of the responses received to specific questions. Please note that most private sector respondents elected to remain anonymous, while a number of the respondents who were prepared to be named indicated that their responses may not be attributed to their institution. No respondents are therefore named in this discussion.

3.1 Client identification and verification measures as barriers

Question: *Are there clients who are unable to meet your client identification and verification requirements that apply to financial inclusion and other products?*

a. If so, what are the general reasons why they are unable to meet the requirements?

b. What percentage of potential clients would be negatively affected by the requirements?

The general responses were positive and very few institutions reported that they needed to turn away significant numbers of citizens who were unable to meet the client identification and verification requirements. Problems were however noted in relation to certain informal institutions such as rotating credit schemes and foreign citizens, especially asylum seekers and refugees.

3.2 Politically Exposed Persons (PEPs)

Question: *Do you apply measures to determine whether prospective clients are Politically Exposed Persons? If so, please describe the measures and the means by which you access the relevant information. If not, please elaborate.*

The responses represented a broad range of practices, depending on whether national laws required steps to be taken:

1 Large financial institutions, especially those that operated internationally or were part of international groups reported in general that all clients are screened against one or more commercial databases to determine whether they are PEPs.
2 A number of smaller institutions reported that they ask each client during account-opening whether that person is a PEP and whether they implement PEP risk management measures when the client answers positively. In some cases institutions indicated that their staff members know the national PEPs and are able to identify them without additional assistance.
3 Some institutions reported that they do not implement PEP measures at all without explaining why none were implemented. Others indicated that they have not implemented such measures because they deem them discriminatory or because they deem the measures inapplicable to their clients who are mostly low-income clients. A number of institutions reported that they have not implemented measures because PEP measures are not required in terms of the AML/CFT law of the country concerned.

3.3 Implementing targeted financial sanction regime of the United Nations Security Council

Question: *Do you scan client and parties to transactions to identity whether any are subject to United Nations Security Council sanctions in relation to terrorist financing or proliferation of weapons of mass destruction If so, please describe the measures and the means by which you access the relevant information. If not, please elaborate.*

The responses represented a broad range of practices:

1 Large, international institutions often used two screening applications(one for payments and for clients) to ensure that business is not done with listed persons. Screening is normally done against commercial databases that are updated at least daily.

2 Smaller institutions reported downloading lists from the OFAC website and using them to screen their customers. A few reported that they relied on lists, primarily UNSC lists, circulated by their regulator.

3 Some screened only cross-border transactions against sanction lists and not all banks apply sanctions screening measures at account opening. Screening, when it occurs, is generally done manually by smaller institutions. Accounts, when screened by these institutions, were generally screened monthly.

4 A few disclosed that they do not have access to any sanctions lists and do not implement any sanctions controls. One institution reported that their transactions and account balances are so small that they do not pose any money laundering or terrorist financing risk.

3.4 Product risk assessment

Question: *Do you assess the risks of your products being abused for money laundering or terrorist financing? If so, can you describe your risk assessment processes? If not, please elaborate.*

Large financial institutions reported that their products are assessed with reference to the factors such as:

- The way in which services are delivered to clients (eg. branch interface, internet access);
- Transaction value, flow and frequency ;
- Type of client usually associated with the product;
- International standards and trends;
- Local industry trends;
- Fraud incidents involving the product; and
- Local regulatory standards.

In addition, large financial institutions take note of the number of suspicious transactions related to specific products as well as access to information pertaining to the client (corporate, informal body etc.) at whom a product is targeted.

New products are normally subject to a new product approval process where the risks posed by the product are discussed and assessed before sign-off and implementation.

Smaller institutions on the other hand did not report any risk assessment processes or did not provide any further information on their processes.

3.5 Client risk assessment

Question: *Do you assess the risks of money laundering and terrorist financing posed by your clients? If so, please describe the processes and the information that you consider in the assessment process. If not, please elaborate.*

Larger institutions reported that they had sophisticated client-risk assessment processes and models that are often closely linked to product risk assessments, such as higher risk levels if a client used a higher-risk product. Risk scoring is often automated and client grading may change from month to month. Clients are generally assessed with reference to factors such as:

- Type of client;
- Geographical location;
- Occupation or source of income;
- Client segmentation;
- Delivery channels for products and transactions; and
- Employment.

In addition, PEP checks are performed that may lead to a higher risk assessment where a client is found to be a PEP.

Some smaller institutions on the other hand have very basic client-risk assessment processes while many institutions did not report having any ML/FT client risk assessment processes. A few reported having assessment processes but these seem to amount to little more than indicators of suspicious activity that should be reported, or monitoring processes that underpin suspicious transaction reporting.

3.6 Suspicious transaction report (STR) trends

Question: *If you do have an obligation to report suspicious transactions, have you filed any suspicious transaction reports in respect of:*

a. *financial inclusion products or services; and/or*
b. *other products or services (i.e. products aimed at clients who are not low income persons and who have or use other formal financial products)?*

If so,

a. *What were general grounds for the suspicions that were raised in relation to both groups of products and services?*
b. *Were there any differences between the grounds for suspicion relating to financial inclusion products or services compared to those in relation to other products or services?*
c. *What was the ratio of reports filed per number of financial inclusion products or services (for example 1 per 1000 accounts/ transactions/customers, depending on your data capturing processes)?*
d. *What was the ratio of reports filed per number of other products or services?*

Many institutions reported that they have not yet filed any STRs for either financial inclusion or standard products. Where reports were filed in relation to both products, the reasons for suspicion appeared to be fairly similar and mainly related to activities inconsistent with the client or product profile or identity fraud.

In general however, those institutions that have both groups of products and have filed reports, filed proportionally far fewer STRs for financial inclusion products than for standard products. For example, one institution reported filing on average one report per 15,700 financial inclusion accounts over the 30-month period preceding the survey while an average of 1 in 2 200 reports were filed in relation to standard products. Another institution another country reported filing one report per 20 000 financial inclusion clients while filing six reports per 20 000 standard clients. A third institution reported filing one report per 1,000 financial inclusion accounts and two reports per 1,000 standard accounts.

While this reflects the general trend when financial inclusion and standard products are compared, one large international bank pointed out that a particular national financial inclusion product generated a disproportionately high number of alerts per month compared to individual standard products (i.e. not standard products as a group). The apparent cause seems to be that the financial inclusion product is used as a vehicle for advance fee and other related scams.

Most institutions that have filed reports in relation to both types of products were not able to provide comparative data as such data is not collected.

3.7 Identity fraud

Question: *Have any of your clients attempted to commit identity fraud in relation to any of your products or services? If so, please describe the types of offences, the number of instances and how they were detected.*

A number of institutions reported cases of attempted identity fraud in relation to their products. Three disclosed the numbers of cases that were identified:

- Bank A (large international bank): On average, 1,000 cases of attempted identity fraud were identified per month from January to April 2012;
- Bank B (large domestic bank): Approximately 250 identity fraud cases per month were detected;
- Bank C (medium-sized domestic financial institution): 129 cases were identified from January to July 2012.

These cases were generally identified by employees, forensic investigators, internal audit functions and fraud detection processes.

3.8 Employee integrity

Question: *Do you have any specific measures to mitigate any money laundering, terrorist financing or fraud risks posed by your employees, for example do you perform integrity checks before employing a person? If so, please describe the processes and the data that you consider in those processes.*

Most institutions reported that they had prospective employee screening processes. Larger institutions generally have more sophisticated systems. Institutions in countries with more extensive data (for example credit bureaus and accessible criminal records) generally have more extensive controls than institutions in countries that lack such data.

Generally the following checks are undertaken:

- A criminal record check;
- Reference checks to previous employers;
- Screening against inter alia UNSC sanctions lists and PEP lists; and/or
- A credit check.

South African institutions generally also run checks against the Register of Employee Dishonesty, a banking industry platform where the names of all employees who were dismissed for dishonesty are posted together with their transgressions.

3.9 Agent integrity

Question: *Do you have any specific measures to mitigate any money laundering, terrorist financing or fraud risks posed by your agents (if any), for example do you perform integrity checks before engaging an agent? If so, please describe the processes and the data that you consider in those processes.*

Not all institutions have agents but those who do reported a range of difference practices relating to agent integrity checks. Some institutions subject agents to the same integrity checks that are applied to prospective employees. Other institutions merely reported that due diligence measures are undertaken while some said that they did not undertake any specific integrity measures in relation to agents. These institutions often relied on the agent agreement and service level agreements, including compliance standards, embodied in that agreement. The agreement allows the institution to terminate the contract if the agent fails to adhere to the agreed standards. One institution claimed that it had a rigorous agent selection process in place but it described an agent identification and verification process that does not provide any level of assurance regarding the integrity of the prospective agent.

3.10 Identifying fake identity documents

Question: *If you require customers to produce documents verifying their identity, do you train employees to identity possibly forged or fake documents? If so, please explain.*

Most institutions reported that they provide some level of training for their employees to enable them to identify fake identification documentation. Some larger institutions reported that their employees are required to subject documents to ultra violet light testing. Employees are trained to:

- Check that photos on identity document match the face of the person in front of them;
- Ensure that names match the gender;
- Scrutinise the photo to make sure it has not been replaced; and
- Scrutinise national documents to ensure that standard security features, such as stamps and holograms, are present,

This is not done by all institutions and processes of smaller institutions do not appear sufficiently rigorous to identify and prevent identity fraud.

3.11 Constructive steps

Question: *Are there any constructive steps that can be taken by the state, the regulator or any other body to assist you to manage financial inclusion and financial integrity objectives better? If so, please elaborate.*

A number of institutions suggested improved channels of communication with national regulators to discuss appropriate and consistent practices. Larger institutions that operate across borders in the region also supported regional engagement. Improvement in national identification infrastructure and access to identification information held by the state was also requested.

4 RECOMMENDATIONS

In view of the responses, three broad sets of Recommendations are made:

- Recommendations for similar studies in the future;
- Recommendations for engaging with ESAAMLG members; and
- Recommendations for engaging with the private sector.

4.1 RECOMMENDATIONS FOR SIMILAR STUDIES IN THE FUTURE

A survey is a helpful tool to obtain data. In this case, however, the subject matter appeared to be too complex for smaller institution to provide appropriate responses. Large banks generally took great care to provide comprehensive information. Many relevant challenges experienced in relation to low-risk financial inclusion products and services may be experienced by the smaller institutions and the responses did not shed sufficient light on these matters to support informed conclusions.

In future, such data can possibly be gathered through on-site visits to, or a national workshop with, representatives of large and smaller financial institutions. It would also be helpful to have one consolidated report presenting national views, as submitted by Namibia, rather than a large number of often conflicting reports from different institutions in a country.

It is recommended therefore that the design of similar studies in future should ideally involve either on-site visits to the relevant parties or national workshops where participants can share and debate their views, informing a consolidated national report that is submitted to ESAAMLG.

4.2 RECOMMENDATIONS FOR ENGAGING WITH ESAAMLG MEMBERS

4.2.1 Supporting the development of national policy and legal frameworks

Despite the fact that all countries that participated in the survey supported various financial inclusion initiatives, most countries lacked a comprehensive policy framework to support financial inclusion and specifically products such as mobile money and prepaid cards and delivery channels such as agency banking and other agent-delivered financial services.

In Bester et al's *Implementing FATF Standards in Developing Countries and Financial Inclusion: Findings and Guidelines*,[12] a report emanating from the ESAAMLG region that provided the first conclusive indications that inappropriate AML/CFT measures can impact negatively on financial inclusion, the authors advised countries that wished to balance financial inclusion and financial integrity to adopt a comprehensive policy framework:[13]

> "Before an AML/CFT regime is enacted or even if already enacted, the domestic financial sector policy-maker or regulator should consider the interaction between imposing AML/CFT controls and financial inclusion. Policy makers should guard against adopting templates or regulations imposed in other jurisdictions without first considering the appropriateness and potential impact of those regulations in their own jurisdictions. It is important to consider financial inclusion in the policy-making process, but ideally the policy should be comprehensive and should also give consideration to other relevant factors such as existing and expected crime patterns, law enforcement, regulatory and compliance capacity, undocumented migration and market and social development conditions."

In addition, Isern and de Koker make the following recommendations in a CGAP *Focus Note* on financial integrity and financial inclusion:[14]

> "Many government agencies and departments are involved in different aspects of the AML/CFT framework and of financial inclusion. The core business of these agencies and departments often give them very different perspectives on AML/CFT approaches, policies, and priorities. To ensure a cohesive approach, the country should adopt a clear, overarching policy that commits the government as a whole to effective and proportional controls. The policy should be comprehensive and reflect the approaches outlined in the following."

In view of the importance of clear and comprehensive policy frameworks to advance financial integrity and financial inclusion, engagement on this topic is important.

It is recommended that the Working Group organises a peer-learning workshop for ESAAMLG members to support the drafting of comprehensive national policy and legal frameworks that would balance financial integrity and financial inclusion policy objectives. Such policies should ideally

- **Align the financial inclusion and financial integrity objectives and programmes of action of the government departments, agencies and regulators involved in different aspects of financial integrity and financial inclusion;**

- **Enable the development of legal and regulatory frameworks that permit risk-based implementation of the FATF standards, especially for appropriate new payments systems and new service delivery channels;**

---

12 Bester, Chamberlain, de Koker, Hougaard, Short, Smith, and Walker *Implementing FATF Standards in Developing Countries and Financial Inclusion: Findings and Guidelines* FIRST (2008) World Bank, Washington DC.

13 Bester, Chamberlain, de Koker, Hougaard, Short, Smith, and Walker *Implementing FATF Standards in Developing Countries and Financial Inclusion: Findings and Guidelines* 31.

14 Jennifer Isern and Louis de Koker "AML/CFT: Strengthening Financial Inclusion and Integrity" *CGAP Focus Note* 56 (2009) 5.

- **Empower regulators to assess money laundering and terrorist financing risks of new payments systems and new service-delivery channels and advise appropriate controls that balance financial inclusion and financial integrity objectives; and**

- **Respond appropriately to national opportunities and address the objectives and challenges of service providers and vulnerable users.**

4.2.2 Simplified CDD for cross-border transactions and services

None of the countries that participated in the survey allow simplified CDD for cross-border financial services.

Given the current levels of cross-border money flows in the ESAAMLG region and the objectives to increase economic integration, it is worth considering whether general frameworks for simplified CDD in relation to cross-border financial services should be developed. This is a matter that national regulators should consider jointly. Frameworks may provide simply for communication between relevant regulators when providers approach a regulator in one country with a proposed product or service. They may also extend to a more detailed tiered system that would enable providers to develop a range of different products within the different risk-based parameters set by regulators jointly for such services in the region. For general financial services, such frameworks should ensure compliance with the FATF standards for simplified CDD, while the FATF standards for remittances should be met in relation to cross-border remittances.

It is recommended that the Working Group should

(3) Investigate whether there is a need for appropriate simplified CDD in relation to cross-border financial transactions amongst ESAAMLG member countries; and, if so

(4) Advise the Ministerial Council on the most appropriate ways to ensure that appropriate proportional controls are imposed where risk is lower.

4.2.3 Risk assessments

Most countries that participated in the survey are considering or planning to undertake a national ML/FT risk assessment while Namibia was in the process of undertaking its assessment. Many countries are grappling with the complexities of undertaking an ML/FT risk assessment. An important opportunity exists for peer learning in this regard in ESAAMLG regarding the methodology of such an assessment.

It is recommended that the Ministerial Council requests each member of ESAAMLG to file a report with ESAAMLG within six months of completing its initial risk assessment, sharing

its risk assessment methodology, the challenges it encountered when undertaking the assessment and proposals to improve its data and processes in future.

It is important to note in this regard that countries may decide to undertake a series of smaller sectoral or focused assessments at different levels rather than one, comprehensive assessment. In that case the country should indicate to the Ministerial Council when it would be able to present a report on its methodology.

Reports may include some of the findings of the assessment, but, given the sensitivity of some of the relevant information, countries will not be compelled to share findings in their reports.

4.3 RECOMMENDATIONS FOR ENGAGING WITH THE PRIVATE SECTOR

Many respondents indicated that they are satisfied with the current national regulatory arrangements and that their current practices do not exclude a significant portion of their prospective clients. Larger, more sophisticated institutions did however express a desire for more engagement with regulators and for regional engagement, especially where they operate in more than one jurisdiction.

Matters that were noted as problematic and that could benefit from attention by the Working Group are:

a) *Simplified due diligence measures*

A number of respondents expressed uncertainty regarding the range of simplified Customer Due Diligence measures that is acceptable to regulators. They requested engagement and guidance to ensure compliance and greater consistency.

b) *Measures to assist specific vulnerable groups*

Institutions requested guidance regarding effective ways to address the plight of excluded clients who are not generally assisted by current national measures, such as undocumented migrants, asylum-seekers and refugees, and in relation to due diligence measures in respect of clients such as rotating credit schemes.

c) *Identification of Politically Exposed Persons (PEPs) and persons subject to United Nations Security Council (UNSC) sanctions*

While large institutions access commercial databases with the required PEPs and sanctions data, smaller institutions often do not have access to such data and many have no measures in place to ensure adherence to international standards. The lack of national legal and regulatory measures regarding these international obligations is also noted. The relevance and fairness of these measures are also questioned by a number of smaller institutions in relation to their low-income client base. Guidance is required

regarding appropriate access to relevant data and in relation to appropriate compliance measures.

d) Product and client- risk assessment

Large, sophisticated institutions reported that they have comprehensive product and client ML/FT risk-assessment processes. Smaller institutions sometimes have rudimentary processes and, more often, do not undertake any risk-assessment measures at all. Guidance that would enable large institutions in the region to improve their processes and empower smaller institutions would be very helpful.

e) Monitoring of risk levels

Many institutions that have classified products as low-risk products and have filed suspicious transaction reports in respect of those products have often been unable to provide any statistics on the number of such reports that were filed, compared to the number of reports filed in terms of standard- and higher-risk products. Monitoring of risks posed by products that were classified as low-risk is important to ensure that the initial classification was correct. Guidance on the appropriate monitoring and management of risks posed by low-risk products and clients will be helpful.

f) Combating identity fraud in relation to low- risk products

Identity fraud may be easier to commit in relation to products that are subject to simplified, less rigorous due diligence measures. A number of institutions reported that such attempts to commit identity fraud were detected. It would be helpful to have guidance on effective anti-fraud measures in relation to products that are subject to simplified due diligence measures.

g) Integrity measures in relation to employees and agents

It is important that institutions take appropriate steps to ensure that employees and agents do not pose an integrity risk. Large institutions tend to take more extensive steps and these measures tend to be more comprehensive in relation to employees than to agents. Guidance on appropriate management of these risks may be helpful to larger and smaller institutions.

h) Guidance and training on identification of fake documentation

The integrity of documentary verification processes depends on the ability of agents and employees to identify fake documents. While large institutions provide training to their employees and agents to identify fake documents, this is not necessarily done by smaller institutions. Awareness programs, supported by technical information regarding security features of standard government documentation as well as guidance on anti-fraud processes and measures, are required to support the integrity of Customer Due Diligence Processes.

i) Access to national identification data

Customer due diligence measures are easier and cheaper to implement in countries where private providers can access national data to verify identities of clients. Probing the needs of such providers, the ability of countries to provide access to relevant data, and general rules relating to such access will be relevant to advance the alignment of financial inclusion and financial integrity.

While the respondents indicated that more discussion of and guidance on the matters listed in a) – i) above will be of value, it is not clear whether such discussions and guidance should be regional or national. Respondents from different countries highlighted different matters. Given the general inconsistency in answers and the lack of comprehensiveness of many of the surveys, the picture is not clear.

The following is therefore recommended:

Each Working Group member should review the private sector reports submitted by the institutions of their countries and engage the respondents as well as other stakeholders to determine which of the matters above should be addressed nationally and which should rather be addressed regionally, and report their findings to the Working Group;

If appropriate topics for regional guidance are identified, the Working Group should engage private sector representatives at a regional workshop to:

a) **Map potential guidance in relation to the identified matters;**
b) **Design processes, potentially by working in multi-disciplinary working groups, to produce draft guidance relating to appropriate practices; and**
c) **Submit draft guidance to the Ministerial Council of the ESAAMLG for approval.**

September 2013