

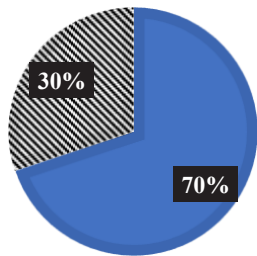
### 3. BANKING SECTOR VULNERABILITY ASSESSMENT

Figure 1: Highlights of the Banking Sector Vulnerability Assessment (as at 31.12.2022)

#### Composition of the Banking Sector

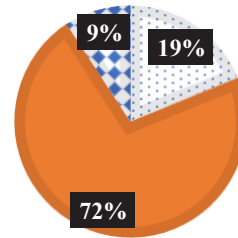


#### Composition of Assets of the Financial System

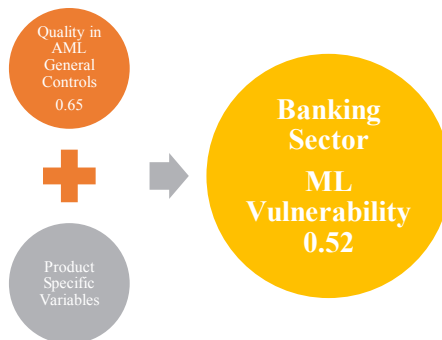


■ Banking Sector ■ Other

#### Composition of Assets in the Banking Sector



■ LCBs ■ LSBs ■ Central Bank



#### Quality in AML General Controls (0.65)



#### Product Specific Variables



### 3.1 Introduction

The banking sector of Sri Lanka is regulated by the Bank Supervision Department (BSD) of the CBSL and, it comprises LCBs and Licensed Specialized Banks (LSBs). The banking sector dominates the financial system of the country, and it accounts for the highest share of the total assets in the financial system. As per Central Bank Annual Report 2022, as of end 2022, the total assets of the banking sector is 61.9 per cent of total assets of the financial system. By end of 2022, the banking sector comprised 30 banks, i.e., 24 LCBs including 11 branches of foreign banks, and 6 LSBs.

### 3.2 Overall Sector Assessment

ML vulnerability of the banking sector is assessed based on the variables provided by the tool i.e., AML general control variables and product specific variables. Accordingly, the ML vulnerability encompasses weaknesses in AML general controls and product<sup>1</sup> specific controls. The general AML controls apply to the entire banking sector and the variables were assessed at sector level. This type of input variables relates to the quality and effectiveness of general AML controls, and therefore affects the vulnerability of all the products being assessed. Whereas the product specific variables affect only particular product. They therefore only impact the vulnerability of the product they are related to.

Accordingly, weaknesses and deficiencies in the areas of quality of the CDD framework arising from a low level of availability of independent information sources and BO information were identified. Further, enforcement of criminal sanctions is observed to be lower.

Considering the overall vulnerability of the products/ services offered by the banking sector, despite the lower prevalence in Sri Lankan banking system, private banking has been identified as the most vulnerable product. This is followed by foreign currency accounts, deposit products, correspondent accounts and electronic fund transfers, all having a medium level of vulnerability.

Accordingly, the overall banking sector vulnerability to ML is rated **Medium**.

### 3.3 Information Collection Methodology

Primary data capture for the assessment primarily involved the use of questionnaires, which were distributed to all banks. Secondary information was gathered from examination reports, supervisory findings, and other reports submitted by banks to the BSD. The assessment was carried out with the assistance of the BSD and representation from Banks.

### 3.4 Quality of Anti Money Laundering General Controls of the Banking Sector

The assessment of AML general controls' quality took into account of 13 general input variables, which are summarized in Table 1 below. A higher rating indicates stronger controls. These variables also impact the vulnerability of all banking sector products and the overall vulnerability of the sector as a whole.

---

<sup>1</sup> The assessment includes products (e.g., deposit accounts), services (e.g., asset management), or channels (e.g., electronic banking). For simplicity, this document will subsequently refer only to products. This reference should be understood as products, services, or channels.

The ratings assigned to the aforementioned 13 AML general input variables are elaborated in detail below.

**Table 1: Anti Money Laundering General Input Variables – Banking Sector**

Banking Sector	Assessment Rating
<b>A. GENERAL INPUT VARIABLES</b>	
Availability and Effectiveness of Entry Controls	High
Comprehensiveness of AML Legal Framework	High
Effectiveness of Supervision Procedures and Practices	High
Availability and Enforcement of Administrative Sanctions	High
Availability and Enforcement of Criminal Sanctions	Medium
AML Knowledge of Banks' Staff	High
Integrity of Banks' Staff	Medium High
Effectiveness of Compliance Function	High
Level of Market Pressure to Meet AML Standards	Very High
Effectiveness of Suspicious Activity Monitoring and Reporting	High
Availability and Access to Beneficial Ownership Information	Medium
Availability of Reliable Identification Infrastructure	Medium High
Availability of Independent Information Sources	Medium

### **3.4.1 Availability and Effectiveness of Entry Controls**

The Monetary Board of the CBSL is the licensing body of banks as per the Banking Act, and through BSD, CBSL effectively carries out its licensing and entry control duties. CBSL and BSD have a clear and comprehensive framework for the licensing of banks including a fit and proper test designed to prevent criminals or their associates holding significant managerial positions in banks. Further, pre-employment vetting is conducted for all bank staff prior to recruitment. These conditions have not changed during the economic crisis period in 2022. Nevertheless, appropriate educational and professional certification for key directors and senior management and availability of adequate AML compliance control requirements are not included in the banking sector licensing framework. Further, availability of a convenient tool for BSD to carry out background checks on key directors and senior management is also lacking in the licensing process and there is no substantial difference in entry controls between foreign banks and domestic banks. Although there are controls in place, considering the above weaknesses, the availability and effectiveness of entry controls was rated as medium.

### ***3.4.2 Comprehensiveness of the Anti-Money Laundering Legal Framework***

Financial Institutions (Customer Due Diligence) Rules, No. 1 of 2016 (CDD Rule) which was issued by the Extraordinary Gazette No. 1951/13 dated January 27, 2016, focusing LBs and LFCs is the main rule on CDD aspect. The FIU also has issued directives, circulars, guidelines as per Section 2(3) of the FTRA to the banking sector to ensure its compliance. Accordingly, the comprehensiveness of the AML legal framework was rated as high.

### ***3.4.3 Effectiveness of Supervision Procedures and Practices***

In order to assess if the banks are complying with relevant legal and regulatory requirements, AML/CFT supervision is carried out by the FIU jointly with the regulator of banks, the BSD, according to the risk based on-site examination plan. The following year's risk based on-site examination plan is drafted based on the outcome of the ML/TF risk assessment conducted by the FIU on all licensed banks annually. The ML/TF risk assessment is conducted using the risk tool developed by the FIU with the technical assistance of International Monetary Fund (IMF). As conducting risk-based supervision examination on banks was initiated in 2016, it was not factored in the NRA 2014. Further, the FIU has taken initial steps to conduct AML/CFT consolidated supervision. In addition, FIU conducts AML/CFT related spot examinations and thematic examinations on banks. Supervisory authorities, i.e., BSD and FIU have well-trained and highly skilled examiners to ensure a high level of AML compliance in the banking sector. Based on the above facts, the effectiveness of AML supervision was rated as high.

### ***3.4.4 Availability and Enforcement of Administrative Penalties***

Section 19 of the FTRA provides for the imposition of penalties relating to non-compliances with AML obligations. Accordingly, the FIU has imposed penalties worth of Rs. 11,750,000 on banks during the year 2022 for violations of provisions of the FTRA and Rules issued thereunder. In instances where shortcomings were identified, such as inadequate AML/CFT enterprise-wide risk assessment, lapses in transaction monitoring systems and CDD process, banks were warned and required to take corrective actions to rectify the deficiencies identified. Subsequently, follow-up examinations were carried out to ensure implementation of recommended corrective actions. Considering the aforementioned facts, the availability and enforcement of administrative penalties was rated as high. Further, as per the feedback received from WG members including compliance officers, it can be determined that administrative sanctions are sufficient to positively influence bank management and staff behaviour.

### ***3.4.5 Availability and Enforcement of Criminal Sanctions***

It can be considered that Sri Lanka has a legal framework that has comprehensive criminal penalties in case of non-compliance with AML Laws and Regulations, as Section 28 of the FTRA prescribes criminal penalties for non-compliance with the FTRA and AML-related offences including offences such as corruption and collusion, and Subsection 3(2) of PMLA contains appropriate criminal penalties for ancillary offences. Based on the feedback received from WG members including compliance officers of banks, it can be concluded that criminal sanctions are effective and sufficiently dissuasive and have a positive influence on the response

and approach of top management of banks. Although banks have not been indicted on ML offences, there are cases where the bank's staff are the main witnesses to prove ML offences. On such instances the bank staff has shown heightened awareness of the penalties that the authorities would impose on violation of PMLA provisions. Further, due to the strict penalties, all banks do take proactive measures to prevent such situations including increased ML/TF training for their staff. Therefore, the availability and enforcement of criminal sanctions with regard to the banking sector was rated as medium.

#### **3.4.6 Anti-Money Laundering Knowledge of the Bank's Staff**

The banks have developed extensive training programmes (both online and classroom) covering AML and CFT laws, policies, and procedures. The frequency of such training programmes can be varied from annual to multiple times during a year based on the size and the requirements of different banks and these programmes are conducted to different categories of bank's staff. Further, most banks have online E-learning platforms, where staff members are required to undertake continuous assessments to update their knowledge on AML/CFT. Also, the staff members have a good knowledge of and are regularly updated on domestic and transnational money laundering typologies, including those involved in the misuse of banks, their products and services. Further, the FIU has been conducting training and awareness programmes for all sectors, specifically for banks consistently to enhance specialized knowledge and skills of their staff. Considering the above facts, the AML knowledge of the bank's staff was rated as high.

#### **3.4.7 Integrity of Bank's Staff**

Comprehensive training programmes have been developed and conducted by the respective banks to uplift the fraud awareness knowledge of the staff members. Disciplinary actions are taken on staff members who are involved in fraud or policy breaches in line with the relevant banks' internal policies. Further, the banks have reported 196 instances of internal theft and fraud to BSD for the year 2022. Loss amount of these reported events amounted to Rs. 1,364.12 million of which Rs. 1,061.22 million has been recovered by the respective banks as at 30.06.2023.

The FTRA contains sufficient provisions to deal with tipping-off, confidentiality and protection from civil and criminal liability. Further, the FTRA provides necessary protection to institutions (reporting entity and supervisory authority) and natural persons (auditor, director, partner, officer, employee, or agent) from criminal and civil liability in relation to any action carried out in terms of the Act or regulations, rules or directions issued thereunder, in good faith.

Also, banks have now implemented speak up platforms for employees and have created an environment where employees feel comfortable in speaking up regarding any issues or concerns. Further, mechanisms have also been created to ensure that staff are able to raise "whistleblowing" cases which are independently assessed and reviewed.

Therefore, considering the developments that have taken place since the last NRA, the integrity of bank's staff was rated as medium high.

### **3.4.8 Effectiveness of Compliance Function of the Banking Sector**

Requirements under Section 14 of the FTRA facilitates that Sri Lanka has a sound and necessary regulatory framework to support AML compliance function. Accordingly, all LBs have an independent officer, mostly at the senior management level as the compliance officer. Further, the knowledge level of the compliance officer and the compliance staff are at a good level and the staff has received both internal and external training. Also, banks have developed internal controls to take disciplinary actions on staff members who breach AML policies and procedures.

Internal AML audits are performed in all banks in line with the existing legislation to test the procedures and systems for AML compliance in line with the provisions of the FTRA. Internal auditors also participate in the awareness sessions conducted by the FIU and separate awareness sessions are also conducted by the FIU for external auditors that help to enhance their knowledge on the FTRA and focus on their responsibilities.

At the same time, representing the entire sector, the banks have formed an Association of Compliance Officers of Banks aiming at ensuring a more effective compliance culture. It is evident that the banks attempt to establish fair and equal market conditions, “a level playing field” for all market players which will in turn support good compliance function of the banking sector.

Considering the above facts, the effectiveness of the compliance function of the banking sector was rated as high.

### **3.4.9 Effectiveness of Suspicious Activity Monitoring and Reporting**

When assessing the effectiveness of suspicious activity monitoring and reporting which was rated as high, it was observed that all banks have implemented transactions monitoring mechanisms systematically, semi systematically or manually in compliance with the CDD Rules. As per CDD Rules, banks are required to monitor all business relationships carried out with their customers on an ongoing basis in order to ensure that all transactions conducted are consistent with the economic profile, risk profile and source of funds of the customer. Accordingly, customer information and transaction details are collected, recorded and monitored through the systems, and there are processes in place to create alerts which would assist banks in detecting suspicious transactions.

Further, the STR reporting process is well established at all banks and the STR scope is covered in training programmes conducted to banks’ staff which enhances the awareness among all staff members. Additionally, the FIU provides red flags to banks, which encompass new typologies, enabling them to detect any suspicious transactions. Prevailing provisions of the FTRA provides protection for all staff members who file STRs which encourage the culture of submitting STRs.

### **3.4.10 The Level of Market Pressure to Meet Anti Money Laundering Standards**

The level of market pressure to meet AML standards was rated as very high as in most instances banks are required to uplift their AML standards mainly due to pressure from its commercial partners such as correspondent banks at the time of establishing business relationships and on an ongoing basis. Furthermore, pressure from rating agencies, international lending institutions, foreign investors and most importantly industry pressure also contribute to the upliftment of the AML standards of banks. Further, certain overseas

clients may also require banks to uplift their AML standards prior to establishing business relationships with the investors and also in maintaining the relationships. The Banks' supervisor confirmed that checks and assessments of correspondent banking relationships are conducted based on specific requirements and when the need arises.

Also, all banks are concerned of the reputational risk and loss of business that may arise due to non-compliance with AML standards both locally and internationally, and therefore continue to invest and enhance the AML standards. Since 2020, FIU has been periodically publishing press releases that provide detailed information about penalties imposed for non-compliance with FTRA provisions. Considering the feedback from WG, discussions at the Banks' Chief Executive Officer's and Chairman's meeting with the supervisor, feedback from Financial System Stability Committee meeting, queries that FIU received periodically based on the press release on penalties imposed by the FIU and face to face progress review meetings between high-level officials of banks and the FIU, it can be stated that this initiative has increased reputational damage forcing banks to avoid non compliances.

#### **3.4.11 Availability and Access to Beneficial Ownership Information**

As per the CDD Rules, banks are required to identify and take reasonable measures to verify the identity of the BOs of their customers, if any. Core Banking Systems used by banks have been updated to capture and maintain BO details. Banks collect BO details through self-declarations obtained at the time of establishing business relationship. Further, banks identify/verify BO details utilizing documents relevant to company incorporations<sup>2</sup> submitted by the account holders. Few institutions such as SEC and Registrar of Companies maintain shareholder details. Banks have access to such databases, however, dedicated access portal to such databases would be convenient.

Awareness has been given to all staff members of banks on the requirement of obtaining BO details. However, instances were noted where the knowledge/awareness among staff on this requirement is varied. Based on the above facts, availability and access to BO information was rated as medium.

#### **3.4.12 Availability of Reliable Identification Infrastructure**

As per CDD rules, banks are required to identify and verify the identity of their customers. In this regard, banks collect information of an official personal identification or any other identification document that bears a photograph of the customer such as the NIC/valid driving license from citizens of Sri Lanka and a valid passport from foreign nationals. From legal persons information on Business Registration Certificate/ Incorporation Certificate is obtained. Since 2021, banks have a process to check the customer information via dedicated web portal provided by DRP. In case of inconsistencies, access to DRP is available for banks to verify information.

Furthermore, it is observed that arrangements are proposed to provide access to databases of Department of Motor Traffic and the Department of Immigration and Emigration for verification of authenticity of Driving License and Passport, respectively.

---

<sup>2</sup> Form 1, Form 40, Form 20, etc. under the Companies Act No. 7 of 2007.

Based on the above facts, availability of reliable identification infrastructure was rated as medium high.

#### **3.4.13 Availability of Independent Information Sources**

Although a reliable independent information source is available through CRIB, obtaining that information to verify the transaction patterns of customers is restricted as information can only be obtained in compliance with CRIB Act. It was also observed that if infrastructure is put in place to provide easy access for banks to independent and reliable information sources to enable them to verify the transaction patterns of customers, it would have a positive effect on customer information databases maintained at banks.

Considering the above facts, the availability of independent information sources was rated as medium.

### **3.5 Quality of Bank Operations and Internal Anti Money Laundering Policies and Procedures**

Based on the tool, the quality of bank operations and internal AML policies and procedures, which are pivotal in determining the overall effectiveness of AML general controls in the banking sector, can be influenced by a combination of 13 AML general control variables discussed above and intermediary variables<sup>3</sup>. These factors collectively impact the quality of AML general control in the banking sector.

Internal AML policies and procedures appear to be more robust compared to actual bank operations due to the direct involvement of the board of directors as well as top management in formulating policies and procedures. Although, the direct involvement of the top management could assist the maintenance of the quality of banking operations at a consistent high level, it is important to note that these operations can be influenced by various internal and external factors, unlike the internal policies and procedures which remain relatively unaffected.

Accordingly, considering both quality of internal AML policies and procedures and bank operations, the quality of AML general controls of the banking sector was rated as medium high with a score of 0.65.

### **3.6 Product/Service Vulnerability**

ML vulnerability emanating from products or services in the banking sector was assessed considering 13 product specific variables<sup>4</sup>. The sample consists of highest vulnerable products as per the previous NRA, to maintain consistency and the new product introduced to the banking sector, special deposit account. Accordingly, the sample included 10 products ranging from private banking, foreign currency accounts, deposit products, electronic fund transfers, correspondent accounts and special deposit accounts. All products other than private banking were offered by banks to its customers.

---

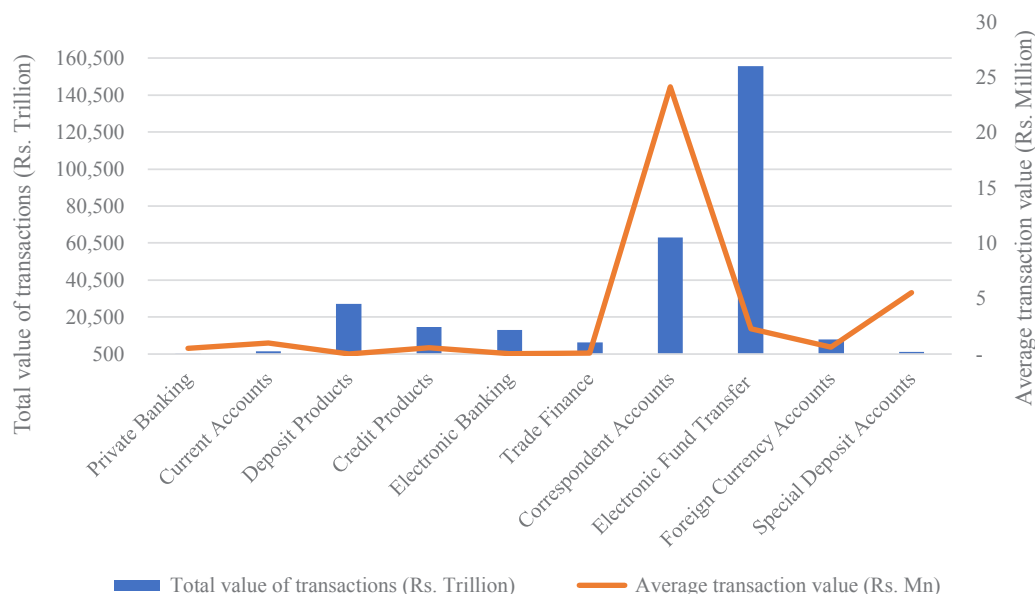
3 Intermediate variables are broad and high-level factors that cannot be assessed directly. They, therefore, need to be disaggregated into their constituent parts in order to be assessed. The module determines intermediate variables automatically, based on the ratings entered for the input variable.

4 Total size/value, Average transaction size, Client base profile, Existence of investment/deposit feature, Level of cash activity, Frequency of international transactions, Anonymous/omnibus use of the product, Existence of ML typologies on the abuse of the product, Use of the product in fraud or tax evasion schemes, Difficulty in tracing the transaction records of the product, Non face to face use of the product, Other factors such as delivery of the product through agents, Availability of product specific AML controls.



Private banking, foreign currency accounts, deposit products, EFTs, correspondent accounts and special deposit accounts were identified as products that are most vulnerable in the ML context and these products ranged around medium level vulnerability. Electronic banking, credit products and current accounts were identified as least vulnerable products in the ML context. These products ranged around medium low vulnerability. Figure 2 below shows the total value of transactions and average transaction size of the product sample during 2016 January - 2021 September.

**Figure 2: Total Value and Average Transaction Size of Products of the Banking Sector during 2016 - 2021**



Source: Licensed Banks

The following section provides a detailed discussion of the products that exhibit a medium or higher level of vulnerability, as derived from the sample.

### 3.6.1 Private Banking

Private banking product is identified as priority banking in Sri Lanka, entails preferential rates, services and reward programmes. It is different from the context of its international banking business in Sri Lanka and it was identified as the most vulnerable product at medium level considering the inherent vulnerability endowed by the tool, high likelihood of PEP remaining among the client base and the amount of cash activity involved in the product. Also, the transaction volumes are comparatively higher irrespective of the low number of customers. However, all private banking customers are subject to normal CDD for which all other customers are subject to and there is no product specific additional CDD measures. Further, enhanced CDD is conducted on high-risk customers including PEP or if any possible ML/TF related risk factor is identified.

### 3.6.2 Foreign Currency Accounts

Considering the facts explained below, the vulnerability of foreign currency account product was rated as medium. Based on the responses received from banks, the volume of transactions of foreign currency accounts is identified as medium level, the average transaction size as low level and the client profile of foreign

currency accounts is identified as a mix of high ML risk clients and low ML risk clients including employees working abroad (non face-to-face), making the client base of medium risk. Further, special mechanisms such as enabling banks to access NIC database, providing banks to get written confirmations from DRP where required, have been established to conduct CDD in respect of non-face to face Sri Lankan customers who are living or employed abroad.

### **3.6.3 Deposit Products**

The deposit products are composed of a mixed clientele, since it caters to the mass market of individual customers, sole proprietorships, large corporates, associations, and clubs. Some are from various jurisdictions. Hence, the client base was rated as high risk in general and the potential for clients using this product to engage in ML does exist but limited. It has a high level of volume compared with the rest of the products in the sample. However, the average transaction size is found to be lower. Therefore, the vulnerability of deposit product was rated as medium.

### **3.6.4 Electronic Fund Transfers**

Considering the below facts, the vulnerability of EFTs was rated as medium. Based on the responses received from banks, the volume of EFTs is found to be high due to the implications of mobility restrictions during COVID-19 pandemic forcing clients to engage in internet banking, average transaction size is found to be medium low in line with the spending pattern of the country and the client profile of the product is identified to be of medium risk. The product involves prominently non face-to-face transactions where customers can instruct banks in writing or electronically to transfer funds to a different account or bank. The small value transactions can mainly be done through Sri Lanka Inter Bank Payment System (SLIPS) and Common Electronic Fund Transfer Switch (CEFTS) systems, and this is mainly used by many institutions for the payment of salaries to their employees. These value transfers are retail in nature.

Further, there are several MVTS providers operating in Sri Lanka such as Western Union, MoneyGram, etc. These MVTS providers have formed partnerships with banks to utilize banks as their remitting partners. When the banks act as the money remitting partners, their licensing requirement is covered under the banking license and Know Your Customer/Customer Due Diligence (KYC/CDD) rules issued to LBs are applicable for the remittance service as well.

### **3.6.5 Correspondent Accounts**

Most of the banks have correspondent relationships with other banks which have strong AML/CFT procedures and systems. All the banking transactions are subject to normal KYC/CDD regulations. Therefore, before establishing the business relationship, CDD is carried out. Enhanced CDD is carried out when dealing with correspondent banks that pose a higher risk, such as those owned by PEPs or banks from high-risk countries. Further, ongoing due diligence is carried out on these relationships. Similarly, banks in other countries carry out CDD on Sri Lankan banks when establishing correspondent banking relationships with them. Further, the average transaction size of correspondent accounts is found to be high, see the Figure 2 above. Considering the above factors, including the comprehensive CDD measures carry out, the correspondent accounts product was rated as medium.

### **3.6.6 Special Deposit Accounts**

Special Deposit Account (SDA) which was rated as medium was introduced as a means of bringing foreign currency held by Sri Lankans in foreign countries to Sri Lankan banking system. A favourable tax system was introduced for SDA. However, normal CDD measures applicable to foreign currency accounts are applicable to SDAs as well. Accordingly, enhanced CDD is conducted on high-risk customers including PEPs or if any possible ML/TF related risk factor is identified.

## **3.7 Ranking of Priority Areas**

The assessment tool ranks the general input variables with respect to their impact on the AML controls and consequently the sector vulnerability. Accordingly, areas have been identified from the assessment that need to prioritize in implementing to strengthen AML controls within the banking sector and those are “Availability and Enforcement of Criminal Sanctions”, “Integrity of Banks’ Staff”, “Availability of Reliable Identification Infrastructure”, “Availability and Access to BO Information” and “Availability of Independent Information Sources”.