Making financial markets work for the poor

AML/CFT and Financial Inclusion in SADC

Consideration of Anti-Money Laundering and Combating the Financing of Terrorism Legislation in Various Southern African Development Community (SADC) countries

Zimbabwe Country Report

Finalised by: Compliance & Risk Resources

March 2015

Contents

ZIMBABWE COUNTRY REPORT

FinMark Trust, an independent trust based in Johannesburg, South Africa, was established in 2002, and is funded primarily by UKaid from the Department for International Development (DFID) through its Southern Africa office. FinMark Trust's purpose is 'Making financial markets work for the poor, by promoting financial inclusion and regional financial integration' as well as institutional and organisational development, in order to increase access to financial services for the un-served and under-served.

While the underlying focus of this report is on the harmonisation and calibration of provisions found in Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) laws and regulations in the Southern African Development Community (SADC), it is hoped that the country reports will become "living documents" that will be used as a resource for SADC Member States to make appropriate amendments to their domestic laws and regulations, define the strategic direction to achieve the objectives of Annex 12 of the FIP and prompt further research and other initiatives that will support State Parties in fulfilling their harmonisation objectives.

FinMark Trust commissioned Compliance & Risk Resources to conduct the final review of the report and to circulate the report to country stakeholders in order to obtain support and facilitate finalisation. The initial research that informed this country report was conducted and prepared by Sarah Langhan and Associates. Raadhika Sihin assisted in reviewing and editing the initial research and country report. She was assisted by a panel of technical experts comprising of Ben Musuku (World Bank), Tom Malikebu (ESAAMLG) and Prof Louis de Koker (Deakin University, School of Law, Faculty of Business and Law) who reviewed and provided guidance on the content for the initial edited research report.

The authors are grateful for the level of cooperation and assistance provided by all persons consulted during the research phase of the project. We especially acknowledge the willingness of those who made themselves available, often at very short notice, in all participating countries to answer questions, provide numerous documents and generally provide the information that was requested. In this regard, we acknowledge and thank all those who assisted.

1. Changes to the Legal and Regulatory Framework Post May 2006

The Eastern and Southern Africa 'Anti-Money' Laundering Group (ESAAMLG) Mutual Evaluation Report was adopted and published in August 2007.[1] The ESAAMLG in-country assessment took place from the 8th of May to the 19th May 2006. The most important development since the ESAAMLG Mutual Evaluation report, which was published in 2008, is the enactment of the Money Laundering and Proceeds of Crime Act, 2013.[2] This new Act repeals the Serious Offences (Confiscation of Profits) Act, 1990 (as amended). Sections 105 to 109 of the new Money Laundering and Proceeds of Crime Act contain important amendments to the Criminal Matters (Mutual Assistance) Act[3], the Suppression of Foreign and International Terrorism Act, 2007[4] , the Building Societies Act[5], the Bank Use Promotion Act (as amended)[6] and the Asset Management Act[7] respectively. The Securities Act[8], although promulgated in 2004, was only operationalised in 2008.

Four sector specific Guidelines were issued by the Bank Use Promotion and Suppression of Money Laundering Unit, namely Guidelines for –

- Money Transfer Agencies and Bureaux de Change (2012);
- The Insurance Sector (2012);
- The Securities Sector (2013); and
- The Real Estate Sector (2014).

These Guidelines are in addition to the earlier Guideline issued in 2006.[9]

Table 1: Zimbabwe: Legislation, Regulation Guidelines (Post ESAAMLG Evaluation)

Year	Legislation and Regulation Enacted and Issued Post ESAAMLG Evaluation
In-country Assessment May 2006 Adopted August 2007	• Suppression of Foreign and International Terrorism Act, 2007 (as amended)[10] • Securities Act, 2004[11] (Operationalised in 2008) Circular No. 1: issued in terms of section 7(1) of the Bank Use Promotion Act (Chapter 24:24), 2004 (Issued 2011) • Circular No. 2: issued in terms of section 7(1) of the Bank Use Promotion Act (Chapter 24:24), 2004 (Issued 2011) • Guidelines on Anti-Money Laundering & Combatting Financing of Terrorism for the Securities Sector, 2013 • Guidelines on Anti-Money Laundering & Combatting Financing of Terrorism for Money Transfer Agencies and Bureaux de Change, 2012

[1] See Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) 2008 *Mutual Evaluation / Detailed Assessment Report Anti-Money Laundering and Combating the Financing of Terrorism: Republic of Zimbabwe.*
[2] Act 4 of 2013.
[3] Chapter 9:06.
[4] Act 5 of 2007.
[5] Chapter 24:02.
[6] Chapter 24:24.
[7] Chapter 24:26.
[8] Act 17 of 2004.
[9] Guideline No. 01-2006 BUP/SML: Anti-Money Laundering. This Guideline applies to all financial and non-financial institutions.
[10] Act 5 of 2007 (as amended).
[11] Act 17 of 2004.

	• Guidelines on Anti Money Laundering & Combating Financing of Terrorism for Insurers, 2012 • Money Laundering and Proceeds of Crime Act, 2013[12] • Guidelines on Anti-Money Laundering & Combating Financing of Terrorism for the Real Estate Sector, 2014 • Suppression of Foreign and International Terrorism (Application of UNSCR 1267 of 1999, UNSCR 1373 of 2001 and Successor UNSCRs) Regulations, 2014 • *New E-Money Guidelines (Draft)*

2. Current AML/CFT Legislation and Regulation in Force in Zimbabwe

Table 2 below provides an overview of the current laws, regulations, exemptions, guidelines and guidance notes in force in Zimbabwe as of June 2014. The legislation is broken up into primary legislation (having a direct bearing on AML/CFT), additional relevant legislation (this covers laws and regulations that impact upon the AML/CFT legal and regulatory framework), laws and regulations applicable to banks, non-bank financial institutions (NBFIs), designated non-financial businesses or professions (DNFBPs), and non-profit organisations. There are two primary pieces of AML legislation currently in force in Zimbabwe, namely the Money Laundering and Proceeds of Crime Act, 2013[13] and the Bank Use Promotion Act, 2004 (as amended)[14]. No Regulations or Exemptions have been issued under the new Act. Four Guidelines issued under the Bank Use Promotion Act, 2004 (as amended)[15] are however applicable. Zimbabwe has a separate counter terrorism Act. The Suppression of Foreign and International Terrorism Act was promulgated in 2007.[16]

Table 2: The AML/CFT Regulatory Landscape in Zimbabwe as of June 2014

	Core Acts		Issued Under the Act	
✓	Money Laundering and Proceeds of Crime Act 4 of 2013		✓	• Guidelines on Anti-Money Laundering & Combating Financing of Terrorism for the Real Estate Sector, 2014
✓	Bank Use Promotion Act, 2004 (as amended) [Chapter 24:24]		✓	• Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism for Financial Institutions and Non-Financial Businesses and Professions 2006 • Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism for Money Transfer Agencies and Bureaux de Change, 2012

[12] Act 4 of 2013.
[13] Act 4 of 2013.
[14] [Chapter 24:24].
[15] [Chapter 24:24].
[16] Act 5 of 2007.

				• Guidelines on Anti-Money Laundering and Combating Financing of Terrorism for the Securities Sector, 2013 • Guidelines on Anti-Money Laundering & Combating Financing of Terrorism for Insurers, 2012 • Circular No. 1: issued in terms of section 7(1) of the Bank Use Promotion Act (Chapter 24:24) of 2004 (Issued 2011) • Circular No. 2: issued in terms of section 7(1) of the Bank Use Promotion Act (Chapter 24:24) of 2004 (Issued 2011)
✓	Suppression of Foreign and International Terrorism Act [Chapter 11:21] (Act 5 of 2007)		✓	• Suppression of Foreign and International Terrorism (Application of UNSCR 1267 of 1999, UNSCR 1373 of 2001 and Successor UNSCRs) Regulations, 2014, Statutory Instrument 76 of 2014
	Additional Relevant Legislation			•
✓	Prevention of Corruption Act [Chapter 9:16] 1996		✗	
✓	Anti-Corruption Commission Act [Chapter 9:22]		✗	
✓	Criminal Procedure and Evidence Amendment Act 2004		✗	
✓	Criminal Law Code		✗	
✓	Companies Act [Chapter 24:03] (1951)		✗	
✓	Companies and Associations Trustees Act [Chapter 24:04]		✗	
✓	Criminal Matters (Mutual Assistance) Act [Chapter 9:06] (1991)		✗	
✓	Extradition Act [Chapter 9:08] (1982)		✗	
	Trafficking in Persons Act, 2014			
	Legislation Applicable to Banks			
✓	Reserve Bank of Zimbabwe Act [Chapter 22:15] (1999)[17]			
✓	Banking Act [Chapter 24:20] (1999)		✓	• Banking Deposit Protection Regulations, 2003 • Banking Regulations, 2000 Statutory Instrument 205 of 2000
✓	National Payment Systems Act [Chapter 24:23] (2001)			

[17]See Reserve Bank of Zimbabwe Amendment Bill, 2009.

	Legislation Applicable to NBFIs				
✓	Securities Act 17 of 2004			✗	
✓	Zimbabwe Stock Exchange Act [Chapter 24:18]			✗	
✓	Building Societies Act [Chapter 24:02] (as amended)			✗	
✓	Asset Management Act [Chapter 24:26]				
	Legislation Applicable to DNBPs and NPOs				
✓	Casinos	Lotteries and Gaming Act [Chapter 10:26] (No. 26 of 1998)		✗	
✓	Lawyers	Legal Practitioners Act [Chapter 27:07] (1981)		✗	
✓	Accountants	Charted Accountants Act [Chapter 27:02] (1918) Public Accountants and Auditors Act [Chapter 27:12] (Act 13 of 1995)		✗	
✓	Precious Metals and Stones Dealers	Precious Stones Trade Act [Chapter 21:06]		✗	
✓	Estate Agents	Estate Agents Act [Chapter 27:17] Act 6 of 1999		✗	
✓	NPOs	Non-Governmental Organisations Act 2004 The Private Voluntary Organisations Act (PVO)		✗	

3. Zimbabwe's Approach to Recommendation 10: Customer Due Diligence (CDD)

CDD requirements are found in sections 15 and 23 of the Money Laundering and Proceeds of Crime Act, 2013[18].

3.1 When is CDD required in Zimbabwe?

Section 15 of the Money Laundering and Proceeds of Crime Act, 2013[19] requires every financial institution and designated non-financial business or profession to identify each one of its customers and verify a customer's identity by means of an identity document when:

- Opening an account for, or otherwise establishing a business relationship with a customer;[20]
- The customer, who is neither an account holder nor in an established business relationship with the financial institution, wishes to carry out a transaction in an amount equal to or exceeding five thousand United States dollars USD5,000 (or such lesser or greater amount as

[18] Act 4 of 2013.
[19] Act 4 of 2013.
[20] Section 15(1)(a).

may be prescribed, either generally or in relation to any class of financial institution), whether conducted as a single transaction or several transactions that appear to be linked, provided that the amount of the transaction is unknown at the time it is commenced, the customer's identification shall be verified as soon as the amount of the transaction has reached the prescribed amount;[21]

- The customer, whether or not he or she is in an established business relationship with the financial institution, wishes to carry out a domestic or international wire transfer or monetary amounts in the amount equal to or exceeding one thousand United States dollars (or such lesser or greater amount as may be prescribed, either generally or in relation to any class of financial institution);[22]
- Doubt exists regarding the veracity or adequacy of previously obtained identity documents[23]; or
- There is a suspicion of money laundering or financing of terrorism involving the customer or the customer's account.[24]

Section 15 of the Zimbabwean Money Laundering and Proceeds of Crime Act, 2013 addresses Financial Action Task Force (FATF) Recommendation 10 specifications. Section 15(1) incorporates all 5 key CDD requirements and, as a "new generation" Act, (passed after the new FATF Recommendations were published in 2012), even contains an exemption for domestic and international wire transfers less than USD1,000 as suggested in the FATF Interpretive Note 16, paragraph 5. It is however important to note that FATF still requires financial institutions to include accurate originator information and a unique account number or reference number in cross-border wire transfers, but stipulates that this information need not be verified for transfers less that USD1,000. The threshold of USD5, 000 set out in section 15(1)(b) for occasional transactions is still well below the threshold of USD 15, 000 recommended by the FATF.

In terms of section 14(1) of the Money Laundering and Proceeds of Crime Act, 2013, no financial institution may maintain any anonymous account or an account under a fictitious name.

In Circular No. 2: issued in terms of section 7(1) of the Bank Use promotion Act (Chapter 24:24) of 2004, the Bank Use Promotion Unit requires financial institutions to establish the ultimate beneficial owner of each transaction or relationship. Further, the identity of the beneficial owner must also be fully established and verified before the bank can engage in business with the person acting on behalf of another.

3.2 Identification measures and verification sources

Section 17 of the Money Laundering and Proceeds of Crime Act, 2013 requires every financial institution and designated non-financial business or profession (to the extent that the required particulars are not disclosed by the identity document in question), to obtain and verify the following particulars in respect of a customer:

- **For a customer who is an individual:** his or her full names and address and date and place of birth[25];

[21] Section 15(1)(b).
[22] Section 15(1)(c).
[23] Section 15(1)(d).
[24] Section 15(1)(e).
[25] Section 17(a).

- **For a legal person:** the corporate name, head office address, identities of directors, proof of incorporation or similar evidence of legal status and legal form, provisions governing the authority to bind the legal person, and such information as is necessary to understand the ownership and control of the legal person[26];
- **For legal arrangements:** the names of every trustee, the settlor, and beneficiary of an express trust, and of any other party with authority to manage, vary or otherwise control the arrangement[27];
- **For a person acting on behalf of a customer:** in addition to the identity of the customer, the identity of any person acting on behalf of a customer, including evidence that such person is properly authorised to act in that capacity[28];
- Information on the intended purpose and nature of each business relationship[29];and
- Sufficient information about the nature and business of the customer to permit the financial institution or designated non-financial business or profession to fulfill its obligations under the Act.[30]

The Money Laundering and Proceeds of Crime Act, 2013 does not specify the reliable, independent source documents, data or information that may be used to verify the identity of the customer.

The first set of guidelines, the Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism for Financial Institutions and Non-Financial Businesses and Professions, issued in 2006 under the Bank Use Promotion Act, 2004 (as amended), state in paragraph 11.9.2 that "the name of individuals residing in Zimbabwe should, during the course of an interview with him, be verified from an original official valid document bearing his/her recent photograph and any of the following may be relied upon:-

(a) National identity cards;
(b) Current valid passports; or
(c) Current valid driver's licenses."

In addition, in terms of paragraph 11.9.6, the current permanent address of the applicant or business must be verified as an integral part of identity. "Satisfactory evidence of address can be obtained by any of the following, a copy of which should be retained, after the original has been sighted. The retained copy shall be duly annotated "original sighted":

(a) A recent paid utility bill.
(b) A recent bank or credit card statement.
(c) A recent bank reference."

The Bank Use Promotion and Suppression of Money Laundering Unit noted that certain customers were excluded from the financial system due to their inability to provide proof of residence. In response to this, Circulars 1 and 2 were issued in terms of section 7(1) of the Bank Use Promotion Act 2004. The dispensation applies to low risk customers and provides alternative options to verify a customer's address, including:
(a) Letters from employers;
(b) Affidavits from landlords;
(c) Third party home owner certificates;

[26] Section 17(b).
[27] Section 17(c).
[28] Section 17(d).
[29] Section 17(e).
[30] Section 17(f).

(d) Letters from schools, chiefs and headman;
(e) Referral letters from Senior Bank Officials;
(f) Letters from a practicing accountant;
(g) Letters from an existing bank customer;
(h) Letters from a practicing doctor;
(i) Letters from a practicing lawyer; and
(j) Letters from a Government Arm.

On-going CDD is required by section 26 of the Money Laundering and Proceeds of Crime Act, 2013[31] which specifically requires financial institutions and designated non-financial businesses and professions to undertake ongoing due diligence with respect to business relationships that are, or may be, subject to the requirements of customer identification and verification including:

- Maintaining current information and records relating to customers and beneficial owners concerned;[32]
- Closely examining the transactions carried out in order to ensure that such transactions are consistent with their knowledge of their customer, and the customer's commercial and personal activities and risk profile;[33] and
- Ensuring the obligations pursuant to high risk customers, politically exposed persons and correspondent banking relationships are fulfilled.[34]

Financial institutions and designated non-financial business and professions are also required to pay special attention to:

- All complex, unusually large transactions, and all unusual patterns of transactions which have no apparent economic or visible lawful purpose;[35] and
- Business relations and transactions with persons including legal persons and arrangements, from or in non-compliant or insufficiently compliant jurisdictions.[36]

With respect to the points above, financial institutions and designated non-financial businesses and professions are required to examine, as far as possible, the background and purpose of these and commit their findings to writing.[37]

3.3 Timing of verification of identity

Section 16 of the Money Laundering and Proceeds of Crime Act, 2013 is titled, "Timing of Customer Identification and Verification" and requires the identification and verification of each customer as well as obtaining the other required information as set out in section 15 of the Act before the opening of an account or establishing a business relationship.[38]

[31] Act 4 of 2013.
[32] Section 26(1)(a).
[33] Section 26(1)(b).
[34] Section 26(1)(c).
[35] Section 26(2)(a).
[36] Section 26(2)(b).
[37] Section 26(2)(c). Section 26(3) further requires that "the findings referred to in subsection (2)(c) shall be maintained as specified in section 24, and shall be made available promptly if required by the Unit or by a foreign counterpart agency, a competent supervisory authority or other authority prescribed by the Minister."
[38] Section 16(1).

However, section 16(1) of the Money Laundering and Proceeds of Crime Act, 2013 states further that the Director may, through a directive, prescribe the circumstances in which the verification of identity may be completed as soon as reasonably practicable after the commencement of business if the risk of money laundering or financing of terrorism is effectively managed and a delay in the verification process is unavoidable in the interests of not interrupting the normal conduct of business.[39]

Sections 16(2) deals with customers and beneficial owners with which the financial institution or designated non-financial business or profession had a relationship before the coming into force of the MLPCA. Section 16(2) requires customer identification and verification of these customers to be done on a risk-sensitive basis depending on the type and nature of the customer, business relationship, product or transaction, or as may otherwise be prescribed in regulations or directives.

Financial institutions or designated non-financial businesses and professions that are unable to fulfill the CDD requirements in Part I of the Act are prohibited from opening an account for or maintaining the business relationship with the customer and are required to immediately report the matter to the Unit.[40]

3.4 Risk-based approach to CDD: Simplified Measures and Exemptions

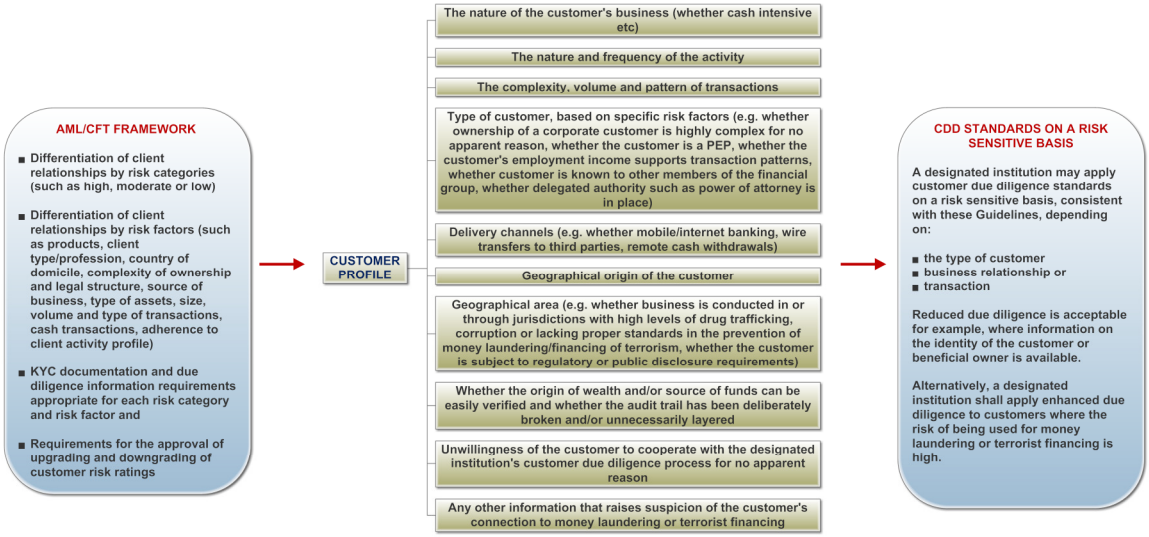
Section 20 of the Money Laundering and Proceeds of Crime Act, 2013 requires enhanced CDD for high-risk customers and politically exposed persons. The Money Laundering and Proceeds of Crime Act, 2013 does not contain any specific sections detailing simplified measures for lower risk customers and products. However, several sections of the MLPCA refer to the application of provisions on a risk sensitive basis depending on the type and nature of the customer, business relationship or products and transactions. Importantly, paragraphs 2.3.7 and 2.3.8 of the Guidelines on Anti-Money Laundering and Combating Financing of Terrorism for Money Transfer Agencies and Bureaux de Change, 2012 which were issued under the Bank Use Promotion Act (as amended), state that:

"A designated institution is allowed to apply reduced or simplified identification measures where the risk of money laundering or terrorist financing is lower. The measures should be documented and must be approved by the board. Where the simplified CDD measures are subject to certain conditions being met, it is necessary to verify that these conditions apply, and where the exemption applies under a certain threshold, measures should be in place to prevent transactions from being split artificially to avoid the threshold. In addition, information beyond customer identity, such as customer location and purpose of the transaction, may be needed to adequately assess risk. This will be an iterative process: the preliminary information obtained about a customer should be sufficient to determine whether to go further, and in many cases customer monitoring will provide additional information."

Paragraphs 2.5.10 to 2.5.25 provide guidance to Money Transfer Agencies and Bureaux de Change on the implementation of a risk-based approach to AML/CFT programmes. Whilst specifically addressed to Money Transfer Agencies and Bureaux de Changes, this guidance is equally applicable to other designated institutions. Diagram 1 below provides a schematic representation of the guidance provided to Money Transfer Agencies and Bureaux de Change on 1) the design of an AML/CFT framework that satisfies the needs of the institution; 2) building a customer profile and; 3) applying CDD measures on a risk-sensitive basis.

[39] Section 16(1)(a) and (b).
[40] Section 22.

Diagram 1: AML/CFT Framework, Customer Profile and CDD on a Risk Sensitive Basis



The threshold exemptions (proven low risk exemptions), implicitly included in sections 15(1)(b) and 15(1)(c) of the Money Laundering and Proceeds of Crime Act, 2013, also have a significant impact upon the financial inclusion agenda in Zimbabwe. As these sections of the MLPCA require every financial institution and designated non-financial business or profession to identify each one of its customers and to verify a customer's identity by means of an identity document when the customer, who is neither an account holder nor in an established business relationship with the financial institution, wishes to carry out a transaction in an amount equal to or exceeding five thousand United States dollars (USD5,000)[41] and when the customer, whether or not he or she is in an established business relationship with the financial institution, wishes to carry out a domestic or international wire transfer or monetary amounts in the amount equal to or exceeding one thousand United States dollars (USD1,000)[42]. It appears that these two sections were drafted in such a manner in order to provide two proven low risk exemptions.

4. Zimbabwe's Approach to Recommendation 11: Record Keeping

Section 24(1) of the new Money Laundering and Proceeds of Crime Act, 2013 requires financial institutions and designated non-financial businesses and professions to maintain all books and records with respect to their customers and transactions, and to ensure that such records and the underlying information are available on a timely basis to the Unit and such other competent authorities as are prescribed by the Minister. At a minimum, the books and records must include:

- Account files, business correspondence, and copies of documents evidencing the identities of customers and beneficial owners obtained in accordance with the Act (to be maintained for not less than five years after the business relationship has ended);[43]
- Records of transactions sufficient to reconstruct each individual transaction for both account holders and non-account holders (to be maintained for not less than five years from the date of the transaction);[44]

[41] Section 15(1)(b).
[42] Section 15(1)(c).
[43] Section 24(2)(a).

- The findings set forth in writing pursuant to section 17(3) *[this must be an error in the drafting as there is no section 17(3) in the Act]* and related transaction information (to be maintained for at least five years from the date of the transaction);[45] and
- Copies of all suspicious transaction reports made pursuant to section 21, including any accompanying documentation (to be maintained for at least five years from the date the report was made).[46]

The Money Laundering and Proceeds of Crime Act, 2013 makes no reference to the manner in which the reports are to be retained.

Where both the Money Laundering and Proceeds of Crime Act, 2013 and the Bank Use Promotion Act (as amended)[47] are silent on the manner in which records should be kept, Paragraph 13.7 of Guideline No. 01-2006 BUP/SML: Anti-Money Laundering states that records of electronic payments and messages must be treated in the same way as any other records. 13.7.2 A comprehensive set of identification documents, in respect of each customer, must be kept in an orderly manner and produced to the Central Bank on request.[48] Paragraph 13.7.3 specifically states that "it is lawful to electronically record any matter and a personal identification mark on the electronically recorded document is as good as a signature."

5. Zimbabwe's Approach to Recommendation 13: Correspondent Banking

Correspondent Banking is comprehensively covered in section 21 of the Money Laundering and Proceeds of Crime Act, 2013.[49] Financial institutions are required when providing cross-border correspondent banking services to:

- Obtain approval from senior management before establishing a correspondent banking relationship, either generally or on a case-by-case basis[50];
- Identify and verify the identification of respondent financial institutions with which they conduct correspondent banking relationships[51];
- Collect all the information which is lawfully capable of revealing the nature of the respondent financial institution's activities[52];
- Evaluate the respondent financial institution's reputation and the nature of supervision to which it is subject[53];
- Evaluate the controls implemented by the respondent financial institution with respect to anti-money laundering and combating the financing of terrorism[54]; and
- Establish an agreement on the respective responsibilities of each party under the correspondent banking relationship to ensure against the risk of money laundering and to combat the financing of terrorism.[55]

---

[44] Section 24(2)(b).
[45] Section 24(2)(c).
[46] Section 24(2)(d).
[47] [Chapter 24:24].
[48] Paragraph 13.7.2 Guideline No. 01-2006 BUP/SML: Anti-Money Laundering.
[49] Act 4 of 2013.
[50] Section 21(a).
[51] Section 21(b).
[52] Section 21(c).
[53] Section 21(d).
[54] Section 21(e).

In the case of payable-through accounts, financial institutions are required to ensure that the respondent financial institution has verified the customer's identity, has implemented mechanisms for on-going monitoring with respect to its customers and, is capable of providing relevant identification information or requests.[56] Section 21 of the Money Laundering and Proceeds of Crime Act, 2013 is supported by paragraphs 11.13 of Guideline No. 01-2006 BUP/SML: Anti-Money Laundering.

In addition, sections 14(2) of the Money Laundering and Proceeds of Crime Act, 2013 prohibits the establishment or operation of a shell bank in the territory of Zimbabwe, and section 14(3) prohibits any person from entering into or continuing a business relationship with a shell bank or a respondent financial institution in a foreign country that permits any of its accounts to be used by a shell bank.

6. Zimbabwe's Approach to Recommendation 14: Money Transfer Services

The Guidelines on Anti-Money Laundering and Combating Financing of Terrorism for Money Transfer Agencies and Bureaux de Change, 2012 were issued under the Bank Use Promotion Act (as amended).[57] Paragraph 2.3.4 of the Guidelines specifically refers to cross-border transactions. Money Transmission Agencies are required to obtain and maintain accurate and meaningful information of:

- The name of the originator;
- The originator account number where such an account is used to process the transaction;
- The originator's address, national identity number, customer identification number, or date and place of birth;
- The name of the beneficiary; and
- The beneficiary account number where such an account is used to process the transaction.

Additionally, the information must remain with the transfer or related messages through the payment chain.[58] Paragraphs 2.3.6, in line with FATF Recommendation 16 (covering wire transfers), covers domestic wire transfers. For domestic wire transfers, the ordering Money Transfer Agency may include full originator information or only the originator's account number or unique identifier, provided that full originator information is available to the recipient Money Transfer Agency and competent authorities within three (3) business days.

---

[55] Section 21(f).
[56] Section 21(g).
[57] [Chapter 24:24]. It is interesting to note that the cover page of the Guidelines states that "the guidelines are issued in terms of the Act and are legally binding, laying down minimum standards on Anti-Money Laundering and Combating Financing of Terrorism (AML/CFT) measures for MTAs and Bureaux de Change" as guidelines issued in other jurisdictions are not legally binding and are used by supervisory authorities as a moral suasion tool.
[58] Paragraph 2.3.5 of the Guidelines on Anti-Money Laundering and Combating Financing of Terrorism for Money Transfer Agencies and Bureaux de Change, 2012.

7. Zimbabwe's Approach to Recommendation 15: New Technologies

Section 25(1) of the Money Laundering and Proceeds of Crime Act, 2013[59] specifically requires financial institutions and designated non-financial business and professions to develop and implement programmes for the prevention of money laundering and financing of terrorism. Such programmes must include "policies and procedures to prevent the misuse of technological developments, including those related to electronic means of storing and transferring funds or value."[60] In addition, section 19 of the Money Laundering and Proceeds of Crime Act, 2013 which deals with situations where customers are not physically present (non-face-to-face transactions), requires financial institutions and designated non-financial businesses and professions to take adequate measures to address the specific risk of money laundering and financing of terrorism in the event that they conduct business relationships or execute transactions with a customer who is not physically present for the purposes of identification.

Importantly, they are required to ensure that CDD measures are no less effective than when the customer appears in person. The section states further that non-face-to-face transactions "may require additional documentary evidence, or supplementary measures, to verify or certify the documents supplied, or confirmatory confirmation from financial institutions or other documentary evidence or measures, as may be prescribed in directives." No directives have been issued on this subject.

Paragraph 11.10 of Guideline No. 01-2006 BUP/SML: Anti-Money Laundering however provides additional guidance on non-face-to-face verification. Paragraph 11.10.2 states that "as with face-to-face verification, the procedures to check identity must serve two purposes: (a) they must ensure that a person bearing the name of the applicant exists and lives at the address provided; and (b) that the applicant is that person." As such, when accepting business from non-face-to-face customers, banks and cash dealers are required to apply equally effective customer identification procedures as for customers interviewed, and additional specific and adequate measures to mitigate the high risk posed by non-face-to-face verification of customers. No guidance is provided on what these specific measures should be. Non-residents applying from abroad are required to complete a standard application form, which is required to incorporate the following:

a) True name;
b) Current permanent address;
c) Mailing address;
d) Telephone and fax number;
e) Date and place of birth;
f) Nationality;
g) Occupation and name of employer (if self-employed, the nature of the self-employment);
h) Passport details, or National Identity Card, Driving Licence or Armed Forces identity Card details (i.e. number and country of issuance), together with issue date and expiry date;
i) Signature/signatures; and
j) Authority to obtain independent verification of any data provided.

As per paragraph 11.10.5 the application form, duly completed must be accompanied by a clearly legible photocopy of any of the following supporting documents:

a) National Identity Card;

[59] Act 4 of 2013.
[60] Section 25(1)(e).

b) Current valid passports;
c) Current valid driving licences; or
d) Armed forces identity card.

This copy must be certified as a true copy by a lawyer, accountant or other professional person who clearly adds to the copy (by means of a stamp or otherwise) their name, address and profession to aid tracing of the certifier, if necessary, and which the bank or cash dealer believes in good faith to be acceptable.

8. Zimbabwe's Approach to Recommendation 16: Wire Transfers

Before the enactment of the Money Laundering and Proceeds of Crime Act, 2013, wire transfers were only covered in Guideline No.01-2006 BUP/SML: Anti-Money Laundering. Wire transfers are now covered in section 27 of the Money Laundering and Proceeds of Crime Act, 2013. The manner in which the de minimis threshold has been included in provides insight into how countries have chosen to interpret the flexibility provided by Recommendation 16.

"Section 27 of the Zimbabwean Money Laundering and Proceeds of Crime Act, 2013[61] reads:

"When undertaking wire transfers equal to or exceeding **one thousand United States dollars,** financial institutions (or such lesser or greater amount as may be prescribed), shall –

(a) Identify and verify the identity of the originator;
(b) Obtain and maintain the account number of the originator or, in the absence of an account number, a unique reference number;
(c) Obtain and maintain the originator's address or, in the absence of an address, the originator's national identity number or date and place of birth; and
(d) Include information referred to in paragraphs (a), (b) and (c) in the message or payment form accompanying the transfer."

Financial institutions are not required to verify the identity of a customer with which it has an existing business relationship, provided that it is satisfied that it already knows and has verified the true identity of the customer.[62]

Section 27(4) of the Money Laundering and Proceeds of Crime Act, 2013 states that "a directive may modify the requirements set forth in subsection (1) –

(a) With respect to domestic wire transfers, as long as the directive provides for full originator information to be made available to the beneficiary financial institution and appropriate authorities by other means; and

(b) With regard to cross-border transfers, where individual transfers from a single originator are bundled in a batch file, as long as the directive provides for the originator's account number or unique reference number to be included, and that the batch file contains full originator information that is full traceable in the recipient country."

Financial institutions that receive wire transfers that do not contain the complete originator information required must take measures to obtain and verify the missing information from the

[61] Act 4 of 2013.
[62] Section 27(2) Act 4 of 2013.

ordering institution or beneficiary.[63] In the event that the financial institution is unable to obtain any missing information, it is required to refuse acceptance of the transfer and report it to the unit.[64]

The Zimbabwean interpretation of Recommendation 16 is interesting in that section 27 of the Money Laundering and Proceeds of Crime Act, 2013 includes the de minimis threshold of USD1,000 but the manner in which section 27 is drafted seems to imply that all wire transfers, be they domestic or cross-border transfers, occasional or regular, that are below the USD1,000 threshold are exempt from the requirements set out in sections 27(1)(a) – (d). This is not the intention behind the exemption for occasional cross-border wire transfers as set out in the Interpretive Note to Recommendation 16."[65]

9. Zimbabwe's Approach to Recommendation 17: Reliance on Third Parties

Reliance on third parties to undertake customer identification is permitted under section 18 of the Money Laundering and Proceeds of Crime Act, 2013 and supported by paragraph 11.12 of Guideline No. 01-2006 BUP/SML: Anti-Money Laundering.

Financial institutions and designated non-financial businesses or professions may rely on intermediaries or other third-parties to perform customer identification as long as:

- There is no suspicion of money laundering or the financing of terrorism;[66]
- Information on the identity of each customer and beneficial owner is provided immediately on opening the account or commencement of the business relationship;[67] and
- The financial institution or designated non-financial business or profession is satisfied that the third party, (i) is able to provide without delay copies of the relevant identity document and other documents relating to the obligation of due diligence upon request, and (ii) it is established, domiciled or ordinarily resides in a compliant jurisdiction.[68]

Importantly, section 18(4) states that compliance with this section does not relieve the financial institution or designated non-financial business or profession relying on the third party from ultimate responsibility for compliance with this Act, including all of the due diligence and reporting requirements thereof.

Circular No. 2: issued in terms of section 7(1) of the Bank Use Promotion Act (Chapter 24:24) of 2004 stresses that when financial institutions rely on introducers, they should carefully assess whether the introducers are genuine office holders and are "fit and proper". Financial institutions should satisfy themselves as to the systems that the introducer has in place to verify the identity of the customer, and conduct periodic reviews to ensure compliance with such systems. The Circular further confirms that ultimate responsibility for knowing customers lies with the financial institutions themselves.

---

[63] Section 27(6) Act 4 of 2013.
[64] Section 27(7).
[65] Langhan and Smith *AML/CFT and Financial Inclusion in the SADC: Investigating the Scope for the Harmonisation of Legislation and Regulation on Anti-Money Laundering and Combating the Financing of Terrorism in Various Southern African Development Community (SADC) Countries* 154 – 156.
[66] Section 18(1)(a).
[67] Section 18(1)(b).
[68] Section 18(1)(c)(i) and (ii).

10. Zimbabwe's Approach to Recommendation 18: Internal Controls

FATF Interpretive Note 18 requires financial institutions' programmes against money laundering and terrorist financing to include (a) the development of internal policies, procedures and controls, including appropriate compliance arrangements and adequate screening procedures to ensure high standards when hiring employees; (b) an ongoing employee training programme; and (c) an independent audit function to test the system. The new Recommendation 18 introduces the requirement that financial groups should have group-wide AML/CFT programmes that include policies for information sharing within the group. Section 25 of the Money Laundering and Proceeds of Crime Act, 2013 is largely compliant with Recommendation 18. Section 25(1) reads:

> "(1) Financial institutions and designated non-financial business and professions shall develop and implement programmes for the prevention of money laundering and financing of terrorism, which programmes shall include the following –
>
> (a) Internal policies, procedures and controls to fulfill obligations pursuant to this Act;
> (b) Adequate screening procedures to ensure high standards when hiring employees;
> (c) Ongoing training for officers and employees to make them aware of this Act and other laws relating to money laundering and the financing of terrorism, with a view to assisting them to recognise transactions and actions that may be aligned to money laundering and the financing of terrorism and to instruct them in the procedures to be followed in such cases;
> (d) Policies and procedures to prevent the misuse of technological developments, including those related to electronic means of storing and transferring funds or value; and
> (e) Independent audit arrangements to review and verify compliance with the effectiveness of the measures taken in accordance with this Act."

Financial institutions and designated non-financial businesses and professions are required to designate a compliance officer at management level to be responsible for the implementation of, and ongoing compliance with, the Act.[69] This Compliance Officer is required to have ready access to all books, records and employees of the institution, business or profession concerned.[70]

In compliance with FATF Recommendation 18 which states that "financial institutions should be required to ensure that their foreign branches and majority owned subsidiaries apply AML/CFT measures consistent with the home country requirements", section 29 of the Money Laundering and Proceeds of Crime Act, 2013 mandates financial institutions to require their foreign branches and majority-owned subsidiaries to implement the requirements of Part I to the extent that domestic applicable laws and regulations of the host country so permit.[71] However, if the laws of the country where the branch or majority-owned subsidiary is situated prevent compliance, the financial institution is required to advise the Unit. The Unit may then take such steps, as it believes to be appropriate, to accomplish the purposes of the Act.[72]

---

[69] Section 25(2).
[70] Section 25(4).
[71] "Part I of this Part" refers to Part I of Chapter III – Customer Identification and Account Opening Requirements.
[72] Section 29(2) of Act 4 of 2013.

As stated previously, Zimbabwe's provisions related to internal controls are largely compliant with FATF Recommendation 18. It however contains no requirements with respect to group-wide AML/CFT programmes.

11. Zimbabwe's Approach to Recommendation 20: Suspicious Transaction Reports (STRs)

Both the Money Laundering and Proceeds of Crime Act, 2013[73] and the Bank Use Promotion Act, 2004 (as amended)[74] contain provisions on suspicious transaction reporting. Section 30(1) of the Money Laundering and Proceeds of Crime Act, 2013[75] requires financial institutions, designated non-financial businesses and professions, and their respective directors, principals, officers, partners, professionals, agents and employees, that suspect or have reasonable grounds to suspect that any property is the proceeds of crime, or is related or linked to, or is to be used for, terrorism, terrorist acts or by terrorist organisations, or those who finance terrorism, to submit promptly (but not later than three working days after forming the suspicion), a report setting forth the suspicion to the Unit. (This obligation also applies to attempted transactions.)

Section 30(4) also requires a competent supervisory authority to inform the Unit if, in the course of discharging its responsibilities, it discovers facts what could be related to money laundering or terrorist financing, or it appears to the supervisory authority that a financial institution or designated non-financial business or profession of which it is the supervisory authority, or any of the respective directors, officers or employees, is not complying or has not complied with the obligations set out in section 30 of the Act.

Section 30(5) of the Money Laundering and Proceeds of Crime Act, 2013 specifically states that "a directive shall prescribe the procedures for and form in which the reports shall be submitted to the Unit" and section 30(6) that "the Unit may supplement the foregoing directive with written guidelines issued from time to time as it sees fit to assist financial institutions and designated non-financial businesses and professions to fulfill their obligations under this section."

To date, no Directives have been issued relating to this provision.

Paragraphs 14 and 15 of Guideline No. 01-2006 BUP/SML: Anti-Money Laundering provides guidance on the recognition of a suspicious transaction and reporting of suspicious transactions respectively. Appendix E provides examples of suspicious transactions. With respect to the format in which suspicious transactions must be submitted to the Unit, the Unit informed us that they currently use a pro-forma form that is emailed by accountable institutions. The Unit apparently did have automated software, but this has not been running.

[73] Act 4 of 2013.
[74] [Chapter 24:24].
[75] Act 4 of 2013.

12. Zimbabwe's Approach to Recommendation 34: Guidance and Feedback

The Bank Use Promotion and Suppression of Money Laundering Unit is established under section 3(1) of the Bank Use Promotion Act (as amended).[76] The Unit's functions are set out in section 4 of the Bank Use Promotion Act (as amended). With respect to guidance and feedback, the Unit is required, in terms of section 4(e) of the Bank Use Promotion Act, 2004 (as amended), to issue guidelines or directions to financial institutions on matters relating to its functions.

FATF Recommendation 34 requires competent authorities, supervisors and SRBs to establish guidelines, and provide feedback, which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and, in particular, in detecting and reporting suspicious transactions.

Five Guidelines have been issued to date. These are 1) Guideline No. 01-2006 BUP/SML: Anti-Money Laundering; 2) Guidelines on Anti-Money Laundering & Combating Financing of Terrorism for Money Transfer Agencies and Bureaux de Change, 2012; 3) Guidelines on Anti-Money Laundering and Combating Financing of Terrorism for the Insurance Sector; 4) Guidelines on Anti-Money Laundering & Combating Financing of Terrorism for the Securities Sector, 2013; and 5) Guidelines on Anti-Money Laundering and Combating Financing of Terrorism for the Real Estate Sector. The Guidelines provide guidance to reporting entities on how to comply with the reporting obligations. For instance: (i) what types of activity may be suspicious; (ii) how to submit an STR; (iii) the rationale for implementing electronic systems to monitor accounts; (iv) transactions related to countries that insufficiently apply AML/CFT measures; (v) prohibitions and restrictions on the right to establish customer relationships with persons from countries that insufficiently apply AML/CFT measures; and (vi) how to obtain further information and assistance concerning these issues.

13. High Level Recommendations for Zimbabwe

The recommendations set out in Table 3 below are not intended to be exhaustive. These high level recommendations provide an indication on how sections in the Money Laundering and Proceeds of Crime Act, 2013[77]and the Bank Use Promotion Act (as amended)[78]could be amended to bring the law in line with the several of the revised FATF Recommendations.

[76] [Chapter 24:24]. It is interesting to note that the cover page of the Guidelines states that "the guidelines are issued in terms of the Act and are legally binding, laying down minimum standards on Anti-Money Laundering and Combating Financing of Terrorism (AML/CFT) measures for MTAs and Bureaux de Change" as guidelines issued in other jurisdictions are not legally binding and are used by supervisory authorities as a moral suasion tool.

[77] Act 4 of 2013.

[78] [Chapter 24:24]. It is interesting to note that the cover page of the Guidelines states that "the guidelines are issued in terms of the Act and are legally binding, laying down minimum standards on Anti-Money Laundering and Combating Financing of Terrorism (AML/CFT) measures for MTAs and Bureaux de Change" as guidelines issued in other jurisdictions are not legally binding and are used by supervisory authorities as a moral suasion tool.

Table 3: High Level Recommendations for Zimbabwe

R10	CDD: Component A - When CDD is Required
Section 15 of the Zimbabwean Money Laundering and Proceeds of Crime Act, 2013[79] is the most compliant provision in the entire SADC region with respect to component (1) of FATF Recommendation 10. Section 15(1) contains all five key requirements listed for when CDD is required and, as a "new generation" Act, (passed after the new FATF Recommendations were published in 2012), contains an exemption for domestic and international wire transfers less than USD1,000 as suggested in the FATF Interpretive Note 16, paragraph 5. It is however important to note that FATF still requires financial institutions to include accurate originator information and a unique account number or reference number in cross-border wire transfers, but stipulates that this information need not be verified for accuracy for transfers less that USD1,000. The threshold of USD5, 000 set out in section 15(1)(b) is still well below the threshold of USD 15, 000 recommended by FATF.	
R10	CDD: Component B - Identification Measures and Verification Sources
It is recommended that the Authorities consider incorporating the content found in the Guidelines with respect to listed independent verification sources into legally enforceable laws and / or regulations.	
R10	CDD: Component C - The Timing and Verification of Identity
Section 16 of the Money Laundering and Proceeds of Crime Act, 2013 is titled, "Timing of Customer Identification and Verification" and requires the identification and verification of each customer and obtaining the other required information as set out in section 15 of the Act before the opening of an account or establishing a business relationship.[80] Section 16(1) states further that the Director may, through a directive, prescribe the circumstances in which the verification of identity may be completed as soon as reasonably practicable after the commencement of business if the risk of money laundering or financing of terrorism is effectively managed and a delay in the verification process is unavoidable in the interests of not interrupting the normal conduct of business.[81] To date, the Director has not prescribed these circumstances. This should be remedied as soon as is reasonably practicable.	
R10	CDD: The Risk-Based Approach to CDD - Simplified Measures and Exemptions
The Money Laundering and Proceeds of Crime Act, 2013 does not contain any specific sections detailing simplified measures for low-risk customers and products. However, several sections of the Money Laundering and Proceeds of Crime Act, 2013 refer to the application of provisions on a risk sensitive basis depending on the type and nature of the customer, business relationship or products and transactions. The threshold exemptions implicitly included in sections 15(1)(b) and 15(1)(c) of the Money Laundering and Proceeds of Crime Act, 2013 also have a significant impact on the financial inclusion agenda in Zimbabwe. As these sections of the MLPCA require every financial institution and designated non-financial business or profession to identify each one of its customers and to verify a customer's identity by means of an identity document when the customer, who is neither an account holder nor in an established business relationship with the financial institution, wishes to carry out a transaction in an amount equal to or exceeding five thousand United States dollars (USD5,000) and when the customer, whether or not he or she is in an established business relationship with the financial institution, wishes to carry out a domestic	

[79] Act 4 of 2013.
[80] Section 16(1).
[81] Section 16(1)(a) and (b).

or international wire transfer or monetary amounts in the amount equal to or exceeding one thousand United States dollars (USD1,000). It appears that these two sections were drafted in such a manner in order to provide two proven low risk exemptions.

R11	Record Keeping

Both the Money Laundering and Proceeds of Crime Act, 2013 and the Bank Use Promotion Act (as amended)[82] are silent on the manner in which records should be kept. Paragraph 13.7 of Guideline No. 01-2006 BUP/SML: Anti-Money Laundering states that records of electronic payments and messages must be treated in the same way as any other records. 13.7.2 A comprehensive set of identification documents in respect of each customer must be kept in an orderly manner and produced to the Central Bank on request.[83] Paragraph 13.7.3 specifically states that "it is lawful to electronically record any matter and a personal identification mark on the electronically recorded document is as good as a signature." It is recommended that authorities consider incorporating the relevant sections in the Guideline into law.

R13	Correspondent Banking

Correspondent Banking is comprehensively covered in section 21 of the Money Laundering and Proceeds of Crime Act, 2013. Section 21 of the MLPCA is compliant with FATF Recommendation 13. Shell banks are covered in section 14 of the MLPCA.

R15	New Technologies

Section 25(1) of the Money Laundering and Proceeds of Crime Act, 2013[84] specifically requires financial institutions and designated non-financial business and professions to develop and implement programmes for the prevention of money laundering and financing of terrorism. Such programmes must include "policies and procedures to prevent the misuse of technological developments, including those related to electronic means of storing and transferring funds or value."[85] In addition, section 19, which deals with situations where customers are not physically present (non-face-to-face transactions), requires financial institutions and designated non-financial businesses and professions to take adequate measures to address the specific risk of money laundering and financing of terrorism in the event that they conduct business relationships or execute transactions with a customer who is not physically present for purposes of identification. These sections are compliant with FATF Recommendation 15.

R16	Wire Transfers

The Zimbabwean interpretation of Recommendation 16 is interesting in that section 27 of the Money Laundering and Proceeds of Crime Act, 2013 includes the de minimis threshold of USD1,000 but the manner in which section 27 is drafted seems to imply that all wire transfers, be they domestic or cross-border transfers, occasional or regular, that are below the USD1,000 threshold are exempt from the requirements set out in sections 27(1)(a) – (d). This is not the intention behind the exemption for occasional cross-border wire transfers as set out in the Interpretive Note to Recommendation 16."

It is recommended that the wording of section 27 be reconsidered.

[82] [Chapter 24:24]. It is interesting to note that the cover page of the Guidelines states that "the guidelines are issued in terms of the Act and are legally binding, laying down minimum standards on Anti-Money Laundering and Combating Financing of Terrorism (AML/CFT) measures for MTAs and Bureaux de Change" as guidelines issued in other jurisdictions are not legally binding and are used by supervisory authorities as a moral suasion tool.

[83] Paragraph 13.7.2.

[84] Act 4 of 2013.

[85] Section 25(1)(e).

R17	Reliance on Third Parties
Section 18 of the Money Laundering and Proceeds of Crime Act, 2013 is largely compliant with FATF Recommendation 18, however no mention is made of the scenario where a financial institution relies on a third party that is part of the same financial group.	
R18	Internal Controls
Zimbabwe's provisions related to internal controls are largely compliant with FATF Recommendation 18. The new law however contains no requirements with respect to group-wide AML/CFT programmes. It is recommended that this deficiency be addressed as soon as is reasonably practicable.	