APRIL 2026

Bank Supervision, Surveillance & Financial Stability Division

AML/CFT/CPF BANKING SECTOR RISK ASSESSMENT REPORT

Table Contents

ACRONYMS

AML/CFT/CPF	Anti-Money Laundering, Countering Financing of Terrorism and Countering Proliferation Financing
ML/TF/PF	Money Laundering, Terrorist Financing and Proliferation Financing
BSSFS	Bank Supervision Surveillance & Financial Stability Division
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
IRA	Institutional Risk Assessment
KYC	Know Your Customer
MLPC	Money Laundering and Proceeds of Crime Act [*Chapter 9:24*]
NPO	Non-Profit Organisation
NRA	National Risk Assessment
PEP	Politically Exposed Person
RBA	Risk Based Approach
STR	Suspicious Transaction Report
UNSCR	United Nations Security Council Resolutions

PURPOSE AND OBJECTIVES OF THE RISK ASSESSMENT

The main objective of the sectoral risk assessment is to identify, assess and understand the ML/TF/PF risks facing each banking institution and the entire banking sector. The risk assessment is part of the risk-based approach, which focuses on identification of high risk institutions, areas and scenarios thus facilitating effective allocation of resources as well as prioritising such higher risk institutions, areas and scenarios.

The risk assessment for the banking sector is conducted after every two (2) years and updated annually if there are material changes in the risk profiles of the banking institutions and the banking sector. This assessment was a review of the ML/TF/PF banking sector risk assessment conducted in March 2025 and it covered the period 1 January 2023 to 31 December 2025.

The results of the risk assessment will inform the supervisory strategies and activities adopted by BSS&FS, including on-site and offsite supervision. It will also inform the frequency and intensity of these activities. Further, the results will inform AML/CFT/CPF policy formulation and strengthening of AML/CFT/CPF frameworks in the country. The emphasis of the assessment was on residual risk.

EXECUTIVE SUMMARY

This report summarises the money laundering, terrorist financing and proliferation financing (ML/TF/PF) risk assessment of the banking sector utilising information as at 31 December 2025. The assessment analysed the inherent risk factors and the controls to determine the residual risk of individual banks and the sector as a whole.

The review of the banking sector ML/TF/PF risk assessment established that the sector is rated **medium** for money laundering, **medium-low** for terrorist financing and **medium-low** for proliferation financing.

Across the 16 banking institutions assessed, the consolidated residual risk ratings encompassing money laundering (ML), terrorist financing (TF), and proliferation financing (PF) were distributed as two (2) High risk, one (1) as Medium-High risk, five (5) as Medium risk, six (6) as Medium-Low risk, and two (2) as Low risk.

Inherent Risk

The banking sector exhibits a **Medium-High** inherent money laundering (ML) risk, attributable primarily to its systemic importance and dominant role in Zimbabwe's financial intermediation landscape, accounting for the majority of domestic and cross-border financial flows. The sector's exposure is further elevated by the presence of higher-risk customer segments, including Politically Exposed Persons (PEPs), as well as inherently higher-risk products and services such as private banking and prepaid cards.

Meanwhile, terrorist financing (TF) risk was assessed as **Medium-Low**, reflecting limited but notable cross-border transactional linkages with jurisdictions associated with terrorist activity risk, coupled with relatively low operational activity in border towns, which predominantly operate on a cash basis.

Proliferation financing (PF) risk was assessed as **Low**, given the limited exposure to individuals, diplomats, or entities designated under United Nations Security Council Resolutions (UNSCRs) related to proliferation financing, and the immaterial transactional activity associated with such parties.

The assessment of the inherent risk factors revealed that size of institution, some customer types, product type, modes of payment and geographies presented sources of vulnerability to ML/TF/PF risks across the banking sector.

The review noted that there is a general understanding of ML/TF/PF risks in the banking sector as evidenced by the banks' institutional risk assessments submitted which identified banks' specific inherent risk factors.

Controls

The assessment noted a significant improvement in board and senior management oversight among the few banks that had been assigned a weak rating in the previous Banking Sector Risk Assessments. This is reflective of a positive direction in promoting a culture of compliance in most banks. However, a few banks had minor deficiencies with regards to board and senior management oversight as reflected by lack of robust deliberations on AML/CFT/CPF issues.

Policies and procedures for most banks covered the key elements of an effective AML/CFT/CPF compliance programme, incorporating AML/CFT/CPF obligations, consistent with the requirements of the MLPC Act and directives issued to banks from time to time.

The majority of institutions had comprehensive KYC/CDD and EDD processes and procedures which cover customer onboarding, risk profiling, and on-going due diligence and escalation procedures on high-risk customers, such as politically exposed persons (PEPs). However, it was established that some banks were not adhering to the provisions of the policies and procedures. The issues noted during onsite examinations, and by internal audit and compliance functions in this respect include missing customer KYC files, failure to conduct ongoing due diligence. Resultantly, supervisory action was taken on such institutions including levying administrative penalties.

The review noted that four (4) of the 16 banks had ineffective transaction monitoring processes and systems largely characterised by manual systems and low level of STRs reporting to the FIU. The monitoring systems were considered ineffective, given the banks' customer base and volumes and values of transactions. Such a scenario exposes the institutions to heightened ML/TF/PF risks. These institutions indicated that they have embarked on projects to enhance their transaction monitoring systems and automate where necessary.

Regarding undertaking of AML/CFT/CPF training activities, the review established that most banks had comprehensive staff training programmes on AML/CFT/CPF, an improvement from the previous risk assessment. Most banks trained boards, senior management and staff on the results of the 2024 Money Laundering National Risk Assessment.

In terms of mitigating TF and PF risks, the review noted that in addition to the above controls, all banks have adequate procedures for UNSCR Sanctions Screening, targeted financial sanctions requirements, including name screening, asset freezing and transaction restrictions.

1. INTRODUCTION

1.1. Section 12A & B of the Money Laundering and Proceeds of Crime (MLPC) Act [Chapter 9:24] (hereafter referred to as "MLPC Act or the Act"), provides for the periodic conduct of the National Money Laundering/Terrorist Financing/Proliferation Financing (ML/TF/PF) Risk Assessment (NRA), and the subsequent conduct of sectoral and institutional risk assessments by competent supervisory authorities and designated institutions (including Banks), respectively.

1.2. The requirement to conduct the risk assessment is part of the risk-based approach (RBA) set out in section 12B of MLPC Act. Risk-based supervision of designated financial institutions entails that the supervisor should allocate more of their supervisory resources (human, material and financial) to institutions and areas they perceive to exhibit high risk. This requires supervisors to identify, assess and understand the ML/TF/PF risks inherent in their sector and implement appropriate supervisory strategies and plans, including onsite examinations and off-site monitoring to mitigate the identified risks.

1.3. The banking sector in Zimbabwe is pivotal to economic growth and development through its financial intermediation role and its link with the global financial system facilitating international payments and receipts. The sector comprises 14 commercial banks, two (2) building societies and one (1) savings bank.

1.4. The sector is characterised by a large customer base, high transaction volumes and values, a large asset base, and a wide range of product and service offerings. These characteristics expose the banking sector to heightened inherent money laundering, terrorist financing and proliferation financing risks.

1.5. The 2024 National Money Laundering Risk Assessment results rated the banking sector as Medium while the 2023 National Terrorist Financing Risk Assessment rated the sector as Low. At the time of this report, the results of the national proliferation risk assessment had not yet been concluded.

1.6. Bank Supervision Surveillance & Financial Stability Division (BSSFS), as the competent supervisory authority for the banking sector, reviewed the sectoral risk assessment in February 2026.

1.7. The risk assessment was conducted to identify, assess and understand the ML/TF/PF risks faced by each banking institution and the sector as a whole taking into account the results of the following national risk assessments:

- 2023 National Terrorist Financing Risk Assessment;
- 2024 Zimbabwe NPO Risk Assessment;
- 2024 National Money Laundering Risk Assessment;
- 2024 Tax Crimes National Risk Assessment;
- 2024 Environmental and Natural Resources Crimes Risk Assessment;
- 2024 Virtual Assets and Virtual Assets Service Providers Risk Assessment; and
- 2024 Legal Persons and Legal Arrangements National Risk Assessment.

1.8. The risk assessment was also conducted to incorporate changes in the Financial Action Task Force (FATF) standards and developments in the operating environment.

Architecture of the Banking Sector

1.9. The composition of the banking sector as at 31 December 2025 is shown in Table 1 below.

Table 1: Banking Sector Architecture as at 31 December 2025.

Type of Institution	Number
Commercial Banks	14
Building Societies	2
Savings Bank	1
Total Banking Institutions[1]	**17**
Non-Bank Financial Institutions Under the Supervision of Reserve Bank	
Credit-only-MFIs	316
Deposit-taking MFIs	7
Development Financial Institutions	4
Total Non - Bank Financial Institutions	**328**
Total Number of Institutions	**345**

[1] Out of 17 banking institutions, one (1) was not assessed as it does not take deposits

1.10. Of the 17 banks, eleven (11) are locally owned and six (6) are foreign owned. As at 31 December 2025, the banking sector had a total of 6.7 million customers and held assets of US$8.04 billion and total deposits of US$4.75 billion.

1.11. Five banks are systemically important, collectively holding 63.72% (US$5.12 billion) of total assets, 66.97% (US$2.91 billion) of loans and advances, and 66.57% (US$3.16 billion) of deposits.

2. METHODOLOGY

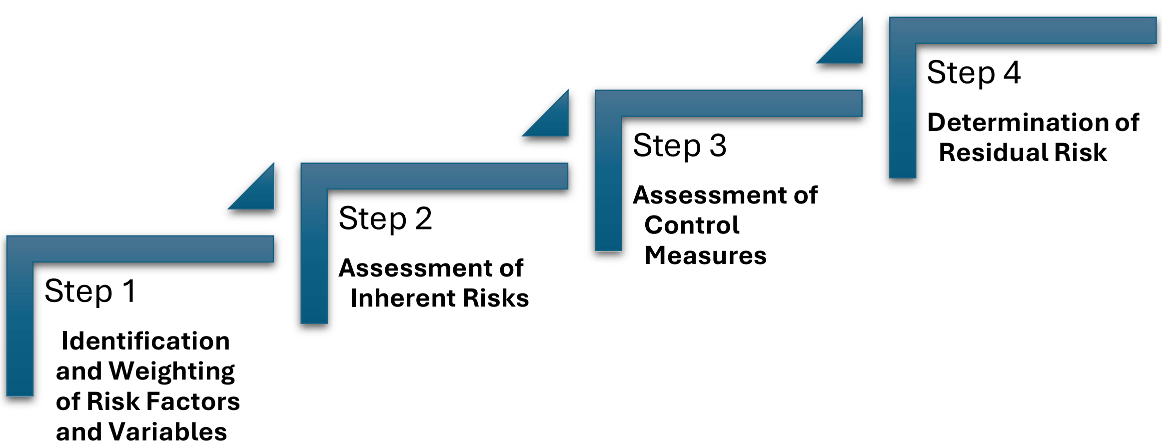
2.1. This assessment adopted the methodology developed by the Financial Action Task Force (FATF), which assesses the risks of money laundering, terrorist financing and proliferation financing (ML/TF/PF) by analysing threats, vulnerabilities and potential consequences. Threats refer to the presence of individuals or groups that may exploit the financial system for illicit purposes, vulnerabilities relate to weaknesses that may be exploited, while consequences refer to the potential impact of such activities on the financial system and the broader economy.

2.2. In applying this methodology, the assessment analysed the inherent ML/TF/PF risks in the banking sector based on key risk factors such as customers, products and services, delivery channels and geographic exposure. The effectiveness of existing control measures was also assessed to determine the residual risk, which reflects the level of risk remaining after the application of mitigating controls.

2.3. Despite the banking sector comprising of 17 institutions, the assessment focused on 16 banks as the other institution is not taking deposits.

2.4. The assessment was a review of the banking sector risk assessment conducted in March 2025. The assessment was conducted using information obtained from banking institutions through questionnaires disseminated to banks, offsite quarterly returns as at 31 December 2025, information from FIU, government publications and results of the various National Risk Assessments indicated above.

2.5. The risk assessment process comprises identification and weighting of risk factors and variables, assessment of inherent risks, assessment of control measures and determination of residual risk as shown in the diagram below.



2.6. Focus group discussions were conducted to select inherent risk factors to be used, relevant control factors and the weightings of the factors and risk categories, taking into account the source, likelihood and impact of the identified vulnerabilities, threats and/or risk factors. The literature on AML/CFT/CPF risk assessment, including FATF publications, International Finance Corporation (IFC) publications, ESAAMLG and Financial Intelligence Unit typology reports and publications from other jurisdictions was also reviewed.

2.7. Analysis of the data and information submitted by banks was conducted using a bespoke ML/TF/PF risk assessment tool focusing on rating of selected inherent risk and control factors for each risk category, that is, ML, TF and PF risk categories.

2.8. The tool made use of embedded formulae to calculate the residual risk, under each risk category, after applying the control factors to the respective inherent risks. The residual risk represents the risk that remains after taking into account existing controls.

2.9. For purposes of designing supervisory strategies, the residual ML, TF and PF risks were consolidated to come up with an ML/TF/PF risk for each institution and the entire sector.

2.10. Inherent risk factors identified were a derivative of the traditional four pillars of ML/TF/PF risk assessment, namely customer, products/services, delivery channels and geography risks. The assessment of inherent risks also considered structural factors, in particular, balance sheet size of the bank (as measured by total assets), total deposits and customer base.

2.11. Control factors were grouped into four (4) categories namely, general ML, TF and PF controls wherein general controls are applicable to the three risk categories.

2.12. The risk assessment used a 5-tier rating scale with the following rating baskets for inherent risk, controls and residual risk; low, medium low, medium, medium high or high, based on the numerical value range as shown in table 1.

Table 2: The Five-Tier Rating Scale

SCORE	INHERENT RISK	CONTROLS	RESIDUAL RISK
5	High (H)	High – Adequate	High (H)
4	Medium high (MH)	Medium High -Almost adequate	Medium high (MH)

SCORE	INHERENT RISK	CONTROLS	RESIDUAL RISK
3	Medium (M)	Medium – Average	Medium (M)
2	Medium Low (ML)	Medium Low - Less than average	Medium Low (ML)
1	Low (L)	Low – Inadequate	Low (L)

2.13. The determination of the residual risk rating is discussed below:

Step 1: Identification and Weighting of Risk Factors and Variables

Identified inherent risk factors and assigned weights to each risk factor to compute the weighted inherent risk score. Information for the identified risk factors was obtained from banks, using questionnaires and quarterly AML/CFT/CPF returns.

2.14. To establish the overall inherent ML, TF and PF risk exposure for each bank, the following proportions were assigned to each risk factor, depending on the likelihood and impact it has to the overall inherent ML, TF and PF risk of the institution.

Table 3: Proportion of Factors and Related Variables

Risk Factor	Proportion
Money Laundering	
Size of the bank (structural factors)	10%
Customers	30%
Products and services	20%
Mode of payments/Delivery channel	20%
Geography	20%
Total	**100%**
Terrorist Financing	
NPO Customers	10%
NPO Credit values	20%
Customers from TF high risk jurisdictions	30%
Values related to TF high risk jurisdictions	40%
Total	**100%**
Proliferation Financing	
Relations with individuals, diplomats, entities designated by UNSCR for proliferation financing (DPRK or Iran)	**100%**

Step 2: Assessment of Inherent Risks

2.15. Assessment of the underlying characteristics of a banking institution that may make it attractive or vulnerable to being used to launder criminal proceeds or to move, store, or generate funds for terrorism or proliferation financing. Higher ratings of these factors were indicative of higher vulnerability of the bank to ML/TF/PF risks. Conversely, lower ratings indicated lower vulnerability of the bank to ML/TF/PF risks.

2.16. The following granular factors were considered for each risk category:

Money Laundering

2.17. **Size of the bank**: the risk factor assessed the banking institutions in relation to their size. The banks were ranked in order of their size and complexity. The proxies used for size were total assets, total deposits and total number of customers, split into individual, legal persons and MSMEs.

i. Large banks have, wider geographical presence, facilitate significant and complex transactions as well as cross-border activities and this heightens their exposure to money laundering risks.
ii. The number of customers is an important factor when assessing how a bank's size relates to money laundering risk, since money laundering is ultimately carried out by customers.
iii. Money laundering risks are generally higher if a launderer can hide proceeds of crime in large and diversified deposit or loan portfolios and may slip through enhanced scrutiny by the bank's systems.

2.18. **Customer type**: the factor assessed whether the type of customers that generally use a banks' products and services increased its exposure to money laundering risks. The following customers were considered to pose higher risk: politically exposed persons (PEPs); high net-worth customers (individuals and corporates); customers from FATF High-Risk Jurisdictions, foreigners and non-resident customers.

i. PEPs are vulnerable to corruption or abuse of power, whilst high net-worth customers may use sophisticated schemes to conceal the origin of funds or hide illicit wealth.

ii. The risk is also considered high for foreign and non-resident customers due to limited access to reliable information for verification of customer identity, source of funds and wealth among other risks.

Additionally, customers in real estate, mining and car dealing sectors were identified to pose higher risks in the 2024 National Money Laundering Risk Assessment and as such were assessed in this review.

2.19. **Products and Services**: assessed the extent to which products and services a bank offers expose it to money laundering risks. The following products and services were considered vulnerable to ML risk as they increase a bank's exposure: pre-paid cards, private banking and trade finance and were indicated as high risk by the Money Laundering National Risk Assessment (NRA) results of 2024.

i. The selected products were considered to pose high risk because of their complexity or lack of transparency and the likelihood that customers might misuse such products for money laundering.

ii. Some prepaid cards do not provide for full KYC information which increases anonymity of the customer. Prepaid cards have high probability of being abused for money laundering and terrorist financing.

2.20. **Modes of payment/Delivery Channel**: - this factor assessed the ways in which customers make payments or transact and the review noted that internet-based payment services are increasingly interconnected with different new and traditional payment services. Each mode of payment poses money laundering risks as they can be used at any of the three stages of money laundering namely, placement, layering and integration. The following are the available modes of payments and were weighted according to the risks they pose: Cash Withdrawals and Cash Deposits (USD Equivalent), Telegraphic Transfers (Incoming and Outgoing), Mobile Banking and Internet Banking. Mobile and internet banking are exposed to cyber risks including cyber fraud.

2.21. **Geography risk:** - assessed the origins and destination of funds transmitted through a bank across its branch network customer location. Geographic location provides an insight into the perceived level of risk associated with branch's location, the country of origin and/or destination.

Border cities/towns, precious minerals mining locations and urban centres were considered to pose high geographic due to proliferation of illegal activities including smuggling, bribery and corruption. Urban centres also serve as fertile grounds for money laundering (ML) due to their dense populations, extensive economic activity, and significant interconnections with global financial centres.

Terrorist Financing

2.22. Four (4) factors were assessed under this category namely, Non-profit Organization (NPO) Customers, NPO Credit values, Customers from TF high risk jurisdictions and Values related to TF high risk jurisdictions.

2.23. NPOs are susceptible to terrorist financing as they may be used as conduits for the collection, movement and disbursement of funds under the guise of charitable, humanitarian or religious activities. The cross-border nature of NPO operations, reliance on cash donations, and activities in conflict or high-risk areas further heighten their vulnerability to abuse.

2.24. Geographic exposure to terrorist financing risk was assessed by considering customers and transactions linked to jurisdictions identified as high-risk for terrorism or terrorist financing.

Proliferation Financing

2.25. Relations with individuals, diplomats, entities designated under the United Nations Security Council Resolutions (UNSCRs), particularly those relating to North Korea (DPRK) or Iran, were used as a factor for assessing the inherent proliferation risk. Institutions that maintain such relationships may be exposed to higher risks of sanctions evasion.

Inherent Risk Weighting

2.26. Information from the questionnaires and quarterly returns was used to determine the absolute risk scores on a scale of 1-5 representing the extent to which each risk factor contribute to a bank's exposure to ML, TF and PF risk.

2.27. To determine the weighted score, proportion assigned to each risk factor (perceived importance) was multiplied by absolute risk scores to compute the weighted risk score.

2.28. The weighted risk scores were aggregated to come up with the inherent ML, TF or PF risk and each bank was then rated as either low (1); medium low (2); medium (3); medium high (4), or high (5).

Step 3: Assessment of Control Measures

2.29. AML/CFT/CPF control measures are the processes, procedures and activities that banks put in place to mitigate the inherent ML/TF/PF risks and to protect against the materialisation of a such risks, or to ensure that potential risks are promptly identified and managed. AML/CFT/CPF controls are applied to the various activities undertaken within banks.

2.30. The activities under this step included assessment of banks' level of compliance with AML/CFT/CPF obligations to put in place effective control measures to mitigate the identified inherent ML/TF/PF risks.

2.31. The following documentation and/or information submitted by banks were analysed:

i. board & management committee packs;
ii. latest ML/TF/PF risk assessments;
iii. latest AML/CFT/CPF policies and procedures;
iv. compliance function organograms, qualifications & experience of compliance personnel;
v. compliance review reports, internal audit annual plans, audits reports on AML/CFT/CPF;
vi. rules and thresholds used or embedded in the transaction monitoring systems;
vii. suspicious transaction reports (STRs) submitted to the FIU;
viii. training programs and registers;
ix. United Nations Security Council (UNSC) sanctions screening procedures.

2.32. To effectively and independently assess controls under each risk category, control measures were put into four (4) groups namely general, money laundering, terrorist financing and proliferation financing controls.

2.33. General controls are controls that are applicable to the three risk categories. The assessment identified nine (9) general control factors, including all elements of the AML/CFT/CPF programs, undertaking of institutional risk assessment and the governance structures in place to manage ML/TF/PF risks. Specific control factors included STRs related to ML, TF and PF and UNSCR sanctions screening. The assessment focussed on the level of effectiveness of the internal control measures to mitigate the identified ML/TF/PF risks.

2.34. Weights were then assigned to each control measure based on the team's perception of its capability to mitigate ML/TF/PF risks.

2.35. Money laundering controls: for the determination of money laundering control factors' ratings, general controls were given a weight of 90%, whilst STRs related to money laundering constituted the remaining 10%.

2.36. Terrorist financing controls: general controls were given a weight of 75%, STRs related to terrorist financing constituted 10% and adequacy of UNSCR sanctions screening related to TF constituted the remaining 15%.

2.37. Proliferation financing controls: general controls were given a weight of 70%, dual use goods monitoring constituted 15%, STRs related to proliferation financing constituted 5% and adequacy of UNSCR sanctions screening related to PF constituted the remaining 10%.

2.38. Table 4 below depicts the control measures that were assessed and the weightings assigned to each of the measures.

Table 4: Controls Rating & Scores

Controls	**Weight**
General Controls	
Board & Management Commitment to AML/CFT/CPF	12%
Undertaking of ML/TF/PF Risk Assessment	15%
Adequacy of the AML/CFT/CPF Policies and Procedures	6%
Adequacy of the Compliance Function	10%
Adequacy of KYC/CDD measures	16%
Adequacy of Transaction Monitoring	12%
Record Keeping	10%
Undertaking of independent testing	5%
Undertaking of AML/CFT Training Activities	4%
Money Laundering	
General Controls	90%
ML related STRs reported to the FIU	10%
Total AML	100%

Controls	Weight
Terrorist Financing	
General Controls	75%
Adequacy of UNSCR Sanctions Screening	15%
TF related STRs reported to the FIU	10%
Total CFT	100%
Proliferation Financing	
General Controls	70%
Adequacy of UNSCR Sanctions Screening	10%
PF related STRs reported to the FIU	5%
Dual Use Goods Monitoring	15%
Total CPF	100%

2.39. Each control factor was assessed for overall design and where possible, operating effectiveness through review of various reports for example compliance reports, audit reports and Board packs.

2.40. The AML/CFT/CPF controls were evaluated and scores ranging from 1 to 5 allocated as depicted in table 4 below.

Table 5: Key for Control Factors Scoring

Score	Description	Narration
5	Adequate/High	The banking institution has policies & procedures which adequately address the requirements of the MLPC Act, directives and circulars, as well as maintaining a robust internal control environment (such as management oversight, internal audit and compliance functions frameworks). The compliance culture of banks in this category is considered very strong. The banking institutions effectively implement available policies and procedures.
4	Largely Adequate/Medium-high	There are minor deficiencies that have been identified which can be corrected during the normal course of business through follow-up actions with management, offsite discussions or during onsite examinations. The bank effectively implements policies and procedures, but there may be a few gaps or challenges that still need to be addressed.
3	Average/Medium	Policies and procedures do not adequately cover all aspects of the requirements of the MLPC Act, directives and circulars, level of board and senior management oversight appear to be inadequate. This rating may also mean, despite the policies and procedures covering all aspects of the law, there were noted gaps in the implementation of the policies and procedures and the institution is not effectively addressing its AML/CFT/CPF obligations.

Score	Description	Narration
2	Largely Inadequate/ Medium-low	There are significant shortcomings in an institution's policies and procedures. The policies and procedures do address some aspects of the law. There is a lack of Board and senior management oversight on AML/CFT/CPF compliance. The institution is generally unaware of its AML/CFT/CPF obligations or is aware but is not effectively implementing effective control measures.
1	Inadequate/Low	There are major shortcomings in the policies and procedures, as they do not reflect the requirements of the law. Board and senior management oversight is considered very poor, and there is deemed lack of political will from the board to implement AML/CFT.CPF measures.

2.41. Higher ratings for control measures reflected robust mechanisms to reduce identified ML/TF/PF vulnerabilities of the banks and lower ratings were indicative of banks' weak internal control environment including inadequate policies and procedures and lack of commitment by the board and senior management to effectively implement the compliance programme.

2.42. Each control measure was assigned a score which was in turn multiplied by the weight that the team would have determined to come up with the weighted rating.

2.43. The overall adequacy of AML, CFT and CPF controls for each banking institution was derived from aggregating the weighted ratings of each control measure.

Step 4: Determination of Residual Risk

2.44. **Residual risk** is the remaining ML/TF/PF risk after a reporting entity has applied controls and processes to reduce the inherent ML/TF/PF risk exposure.

2.45. The residual risk rating is a factor of the inherent risk rating and control measures rating. The assessment used a 5-Tier Risk Assessment Matrix that combines the assessment results of inherent ML, TF and PF risk factors and AML, CFT and CPF controls to calculate the residual ML, TF and PF risk for each bank. The residual risk ratings were as follows; low (1); medium low (2); medium (3); medium high (4) or high (5).

2.46. Table 6 below shows the residual risk rating matrix.

Table 6: Banks' residual risk rating matrix

Key for Residual Risk					
Inherent Risk H	**H**	**H**	**MH**	**ML**	**ML**
MH	**H**	**MH**	**M**	**ML**	**ML**
M	**H**	**MH**	**M**	**L**	**L**
ML	**MH**	**ML**	**ML**	**L**	**L**
L	**MH**	**ML**	**ML**	**L**	**L**
Control Factors	L	ML	M	MH	H

3. KEY FINDINGS

3.1. The banking sector is highly vulnerable to ML/TF/PF due to its large size and importance including relatively large number of customers, legitimacy of both large domestic and international transactions, link with the global financial system, large volume of products and services.

INHERENT RISKS

Money Laundering Inherent Risk

3.2. The money laundering inherent risk for the banking sector was established to be **medium-high**. The rating was mainly driven by the existence of high-risk customers, usage of prepaid cards, large volumes of cash transactions, complex transactions and branches in urban centres, mining and boarder post locations.

3.3. The following factors were considered to come up with the money laundering inherent risk:

Size

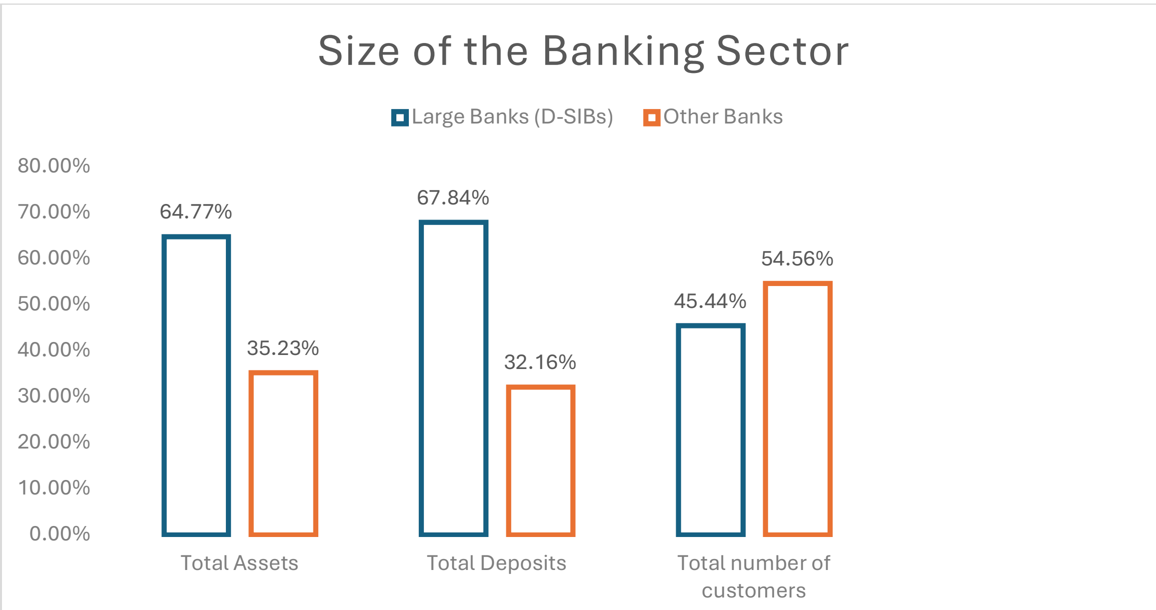
3.4. Large institutions were noted to process significantly higher transaction volumes and values across diverse customer categories and geographic locations. This scale increases exposure to high-risk customers, complex corporate structures and cross-border transactions, while simultaneously placing strain on monitoring systems and compliance oversight.

3.5. The assessment considered total deposits, total assets and total number of customers, disaggregated into individual, corporate and MSME segments, in determining the inherent risk associated with the size of institutions. Of the three indicators, total number of customers was assessed to present the highest inherent money laundering as well as terrorist and proliferation financing risk to the sector, as a larger customer base increases the volume and complexity of transactions, thereby heightening exposure to potential abuse.

3.6. Table below shows how some of the above listed factors were distributed within the sector.

Table 7: Size of the banking sector

	Total Assets (ZWG)	Total Deposits (ZWG)	Total Number of Customers
Large Banks (DSIBs)	135.85 billion	81.84 billion	3.06 million
Other Banks	73.89 billion	38.81 billion	3.67 million
TOTAL	**209.74 billion**	**120.65 billion**	**6.73 million**



3.7. Despite, having fewer number of customers, large banks had the most corporate customers, who pose an elevated money laundering risk due to complex ownership structures, higher transaction volumes and execution of trade finance transactions.

3.8. Of the sixteen (16) assessed banks, forty-five percent (45%), representing seven (7) institutions, were rated medium to high risk in terms of size. These institutions account for a substantial proportion of the sector's total assets, deposits and customers, thereby increasing the potential systemic impact of any ML/TF/PF control weaknesses.

Customers

3.9. The assessment of customer types established that money laundering risk largely emanated from PEPs, high net-worth, foreigners, and customers in the mining sector.

3.10. These customers are characterised as conducting high transaction volumes and values, which are susceptible for money laundering.

3.11. The banking institutions were rated based on the proportion of these high-risk customers to their customer base.

3.12. The sector categorised 52,639 (0.78%) customers as high-risk, 883,662 customers (13.13%) as medium risk and 5.8 million (86.08%) customers as low-risk customers.

3.13. Despite constituting only 0.78% of total customers, high risk customers averaged 20.32% of the banking institutions' transactions, 9.22% of which were from PEPs.

3.14. Meanwhile, seven (7) out of the 16 banks were rated medium to high risk for mining customers. The sector has a high number of foreign customers, however these were mainly concentrated in two (2) out of the 16 banks.

3.15. The table below shows an extract of high-risk customers within the sector.

Table 8: High risk customers

Customer Type	Number	Percentage to Total High-Risk Customers
PEPs	6,944	13.19%
High Net-worth	13,072	24.83%
Foreigners	1,511	2.87%
Mining	5,586	10.61%
Other high-risk customers	25,526	48.49%
Total	**52,639**	**100%**

Products/Services

3.16. The assessment identified trade finance, prepaid cards and private banking as products/services that pose high risk of money laundering in the sector.

3.17. Trade finance presents a high risk of money laundering in banks, emanating from potential over-invoicing of exports, under-invoicing of imports and/or use of fake documents (including fake bills of entry and fake invoices).

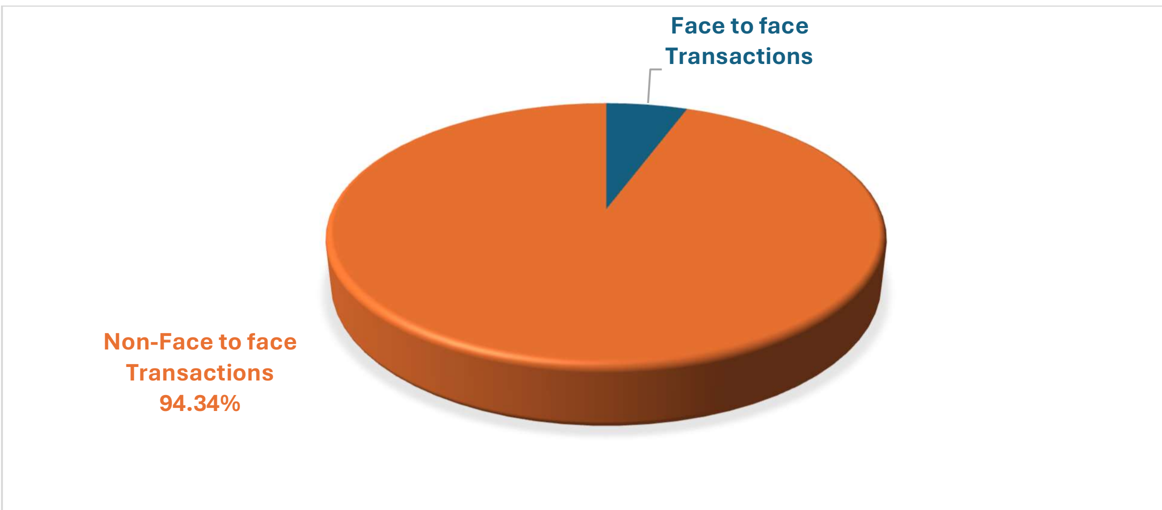
3.18. Prepaid cards were considered high risk as some banks were not collecting adequate KYC information from customers before issuing the cards increasing the risk of the cards being abused to facilitate financial crime.

3.19. The assessment noted that 10 out of the 16 of banks provide private banking facilities to their customers, who constitute 25% of high-risk customers. This product is complex due to its customized nature and is susceptible to abuse through legitimising proceeds of crime (proceeds from corruption or bribery) by the customers.

Delivery channels

3.20. Delivery channels' money laundering risk is driven mainly by cross-border wire transfers and mobile banking services. Their non-face-to-face nature makes them prone to be abused for money laundering purposes.

3.21. The use of mobile and internet banking services was noted to be highly prevalent across all banks due to its flexibility in execution of transactions, with face-to-face transactions only constituting 5.66% of total transactions, as shown in the diagram below:



3.22. Meanwhile, cross-border wire transfers also expose the banking institutions to jurisdictions with weak AML/CFT controls, thereby heightening exposure to money laundering.

Geography

3.23. The assessment established that geography risk mainly emanated from banks' branch networks. Urban centres generally pose high inherent money laundering risk due to high volume and value of transactions, large customer bases and the prevalence of international transactions.

3.24. According to the 2024 National Money Laundering Risk Assessment, mining and border towns exhibited high risk of money laundering due to the prevalence of illegal dealing in precious stones & metals, and smuggling activities. As such, branches located in mining and border towns were identified as posing higher risk of money laundering in this assessment.

3.25. The table below shows distribution of branches between the three (3) identified high risk regions, and as a proportion of the 411 total branches in the sector.

Table 9: High Risk Branches

Geographic Risk Classification	Number of Branches	Percentage to Total Branches
Urban Centres	186	45.26%
Mining Towns	100	24.33%
Border Towns	50	12.17%

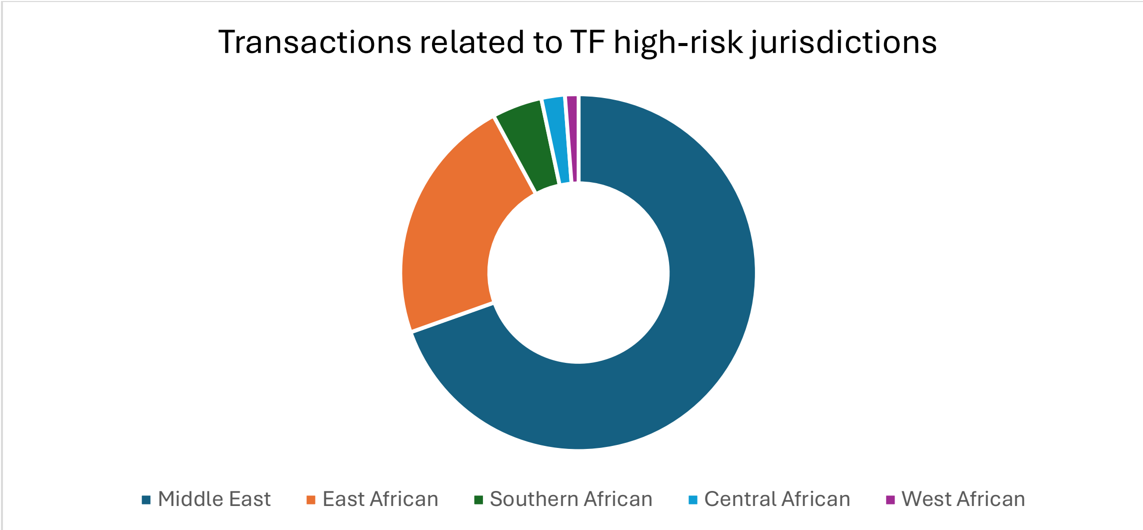
Terrorist Financing Inherent Risk

3.26. The terrorist financing inherent risk for the banking sector was established to be **medium.** The rating was as a result of the presence of Non-Profit Organisations and customers for high TF risk jurisdictions.

3.27. The presents of PEP customers and prevalence of prepaid card use also elevate the sector's TF risk exposure.

3.28. Of the total transactions related to terrorist financing (TF) high-risk jurisdictions, the sector's exposure is concentrated in a Middle Eastern jurisdiction (67.28%), followed by an East African jurisdiction (21.79%), a Southern African jurisdiction (4.38%), a Central African jurisdiction (2.08%), and a West African jurisdiction (1.18%).

3.29. The diagram below shows distribution of transactions related to terrorist financing (TF) high-risk jurisdictions.



3.30. Although transactions linked to the Middle Eastern jurisdiction account for the largest share by value, these emanated from one (1) institution. Excluding the transactions of this institution, the East African jurisdiction becomes the highest contributor, representing 66.10% of the remaining transactions related to TF high-risk jurisdictions.

3.31. Despite having relatively low transactional values, the presence of NPO customers elevates the TF risk as the majority of institutions (15) had NPO customers and these were partly faith-based organisations which were noted to be exposed to higher risks the Sectoral Risk Assessment for Non-Profit Organisations.

Proliferation Financing Inherent Risk

3.32. The proliferation financing inherent risk for the banking sector was rated **low**.

3.33. The rating was a result of absence of banking relationships with individuals, diplomats, consulars, and entities from jurisdictions designated by the United Nations Security Council Resolution for proliferation financing, that is, Iran and the Democratic People's Republic of Korea, as only one (1) out of the 16 institutions had such relationships.

3.34. The rating is further supported by low trade finance transaction which constituted 1% of the total institutions' transactions.

3.35. Notwithstanding, the sector encounters transactions involving dual-use goods which present inherent proliferation financing vulnerabilities, however there has not been any known incidents of abuse of such goods.

CONTROL FACTORS

3.36. The assessment reviewed internal control factors that were considered relevant in mitigating the inherent ML/TF/PF risks. Emphasis was placed on the adequacy and effectiveness of AML/CFT/CPF controls implemented by institutions in line with the AML/CFT/CPF obligations set out in the Money Laundering and Proceeds of Crime Act [Chapter 9:24] (MLPC Act) and related regulations.

Board and Management Oversight AML/CFT/CPF

3.37. The board and senior management of a bank should have oversight on AML/CFT/CPF requirements to foster a culture of compliance within the institution. In particular, the board of directors should put in place a framework to fully identify, monitor and control ML/TF/PF risks.

3.38. The assessment established that most banks had adequate board and senior management oversight to AML/CFT/CPF. This was evidenced by the oversight role of the board is provided for in the banks' policies and procedures and there were notable AML/CFT/CPF deliberations by the main board and relevant board committees.

3.39. Six (6) banks exhibited inadequate AML/CFT/CPF oversight by the board and senior management. The main deficiencies noted relate to delays in remediating and implementing supervisory actions, lack of robust deliberations, as well as absence of board direction and/or involvement on AML/CFT/CPF issues.

Undertaking ML/TF/PF Risk Assessment

3.40. A banking institution should identify, assess and understand its ML/TF/PF risks, in order to put in place appropriate control measures on a risk sensitive basis, in accordance with section 12B of the MLPC Act.

3.41. All banking institutions submitted their institutional risk assessment reports as at 31 December 2025.

3.42. The review of the submitted IRAs noted that several banks; fifteen (15) banks managed to identify, assess and understand the inherent risks facing their institutions

3.43. The risk assessment noted that the institutions were submitting detailed institutional risk assessment reports, taking cognizance of the latest results of the National Risk Assessments, all risk factors, market developments, as well as new products/services.

3.44. Weaknesses noted on the banking institution include not taking into consideration all risk factors and the results of the National Risk Assessments.

3.45. Further, the assessment also established that other institutions did not weigh and score the variables and residual risk, which may result in inefficient allocation of resources.

Adequacy of the AML/CFT/CPF Policies and Procedures

3.46. A banking institution should design and implement comprehensive AML/CFT/CPF policies and procedures to adequately manage the identified inherent risks and ensure compliance with section 25 of the MLPC Act.

3.47. The assessment established that all banks had all the key elements of an AML/CFT/CPF compliance programme in their policies.

3.48. The policies covered KYC/CDD procedures (including Beneficial Ownership), training, record keeping, monitoring and reporting of STRs, sanctions screening, roles and responsibility of board and senior management, the establishment of a Compliance function as well as independent assurance.

Adequacy of the Compliance Function

3.49. A bank should have in place an AML/CFT/CPF compliance function headed by a designated compliance officer or a money laundering reporting officer (MLRO) responsible for AML/CFT/CPF compliance at management level according to section 25 of the MLPC Act.

3.50. The review established that six (6) banks had adequate compliance functions supported by adequate staff resource, appropriate qualifications & experience and appropriate reporting lines.

3.51. There were noted instances where the Head of Compliance reports directly to the Managing Director/Chief Executive Officer, which impairs independence of the function.

3.52. The assessment also noted that some compliance functions had inadequate staffing levels in relation to their size and complexity of transactions.

3.53. Further, some institutions had many open vacancies, and it was also established that some banks Compliance function organograms included compliance champions who are part of business thus potentially posing conflict of interest.

Adequacy of KYC/CDD Measures

3.54. The foundation of any effective system to combat money laundering, terrorist and proliferation financing is the Know Your Customer (KYC) principle and the conduct of Customer Due Diligence (CDD). Sections 15-17 of the MLPC Act require institutions to identify and verify customer information including identification particulars, place of residence, purpose of business, shareholders and beneficial owner of a legal entity and legal arrangement.

3.55. The assessment noted that six (6) banks had comprehensive KYC/CDD and EDD processes and procedures, which cover customer on-boarding, ongoing CDD and escalation procedures on high-risk customers, such as PEPs.

3.56. Weaknesses noted at some banks include absence or inadequate KYC/CDD procedures, non-inclusion of beneficial ownership identification procedures, failure to specify documents required at customer on-boarding and failure to risk profile a customer.

3.57. Further, the assessment noted gaps in KYC documentation including a number of files with missing KYC information in some banks and fraudulent accounts opened using fake KYC documents.

Record Keeping

3.58. Banks should document record keeping and retention procedures, in compliance with section 24 of the MLPC Act.

3.59. It was noted that six (6) banks had comprehensive record keeping procedures in respect of their customers and transactions that contained information on types of documents to be retained and the duration thereof.

3.60. The assessment, however, noted deficiencies in record management, as some KYC files were missing entirely, while others contained incomplete customer records for both individual and corporate clients.

3.61. The record keeping arrangements at some institutions were noted to be inadequate as customer information was not properly secured posing the risk of loss of records.

Undertaking of independent Testing

3.62. Section 25 of the MLPC Act provides for independent review of the compliance programme of an institution and all banks had this provision reflected in their AML/CFT/CPF policies.

3.63. The assessment established that most banks' internal audit functions had conducted independent reviews of their institutions' AML/CFT/CPF programmes in 2023 – 2025 and have internal audit plans that incorporates AML/CFT/CPF audits. The internal audit functions reviewed the key elements of the compliance programme, including governance arrangements, compliance functions, record keeping and training.

Undertaking of AML/CFT/CPF Training Activities

3.64. Training of bank employees and the board of directors is a key component of an effective AML/CFT/CPF compliance program. The design of an effective training programme should take into account the level and nature of the ML/TF/PF risk present in the banking institution and nature of employees' responsibilities.

3.65. The assessment established that all banks had comprehensive training programmes covering AML/CFT/CPF obligations, target groups (employees, management and board) and frequency of training. The assessment also noted that most banking institutions' AML/CFT/CPF policies provide for training of both new and existing staff.

3.66. Most banking institutions maintained training registers, but some of these did not reveal the training programs nor indicate the scope of training employees had received.

3.67. Some banks were not extending AML/CFT/CPF training to their Board members and this may impair their oversight role on AML/CFT/CPF issues.

Adequacy of Transaction Monitoring Procedures

3.68. Transaction monitoring is a key element in the identification and reporting of suspicious transactions to enable investigation and prosecution of ML/TF/PF cases. Sections 26 of the MLPC Act require institutions to perform ongoing customer and account monitoring, to detect suspicious transactions and activity.

3.69. A review of the transaction monitoring procedures revealed that eight (8) banks had adequate transaction monitoring procedures in place.

3.70. 50% of the banking institutions were, however, noted to have manual transaction monitoring systems, which rendered transaction monitoring ineffective, given their size, complexity, customer base and transaction volumes, coupled with inadequate resourcing of the Compliance functions. This was also reflected by reporting low STRs to the FIU by these banks.

3.71. Some banks were noted to have projects related to implementation of automated transaction monitoring systems. These transaction monitoring projects were noted to be outstanding for a long time without much traction.

Identification and reporting of STRs to the FIU

3.72. Banks should have policies, procedures and processes for identifying and reporting suspicious transactions and activities, which are required to be reported to the FIU in terms of section 30 of the MLPC Act.

3.73. The assessment noted that although Suspicious Transaction Reporting (STR) procedures were articulated in most banks' policy and procedure manuals, information obtained from the Financial Intelligence Unit (FIU) indicated instances of non-compliance as some institutions were failing to submit STRs to the FIU.

3.74. It was also noted that some banks (50%) were conducting manual transaction monitoring which resulted in the reporting of low levels of STRs to the FIU.

3.75. Almost all the STRs reported to the FIU were money laundering related with only six (6) relating to terrorist financing and none relating to proliferation financing, during the period 2023 to 2025. This is reflective of low levels TF and PF risks in the sector, and at national level.

3.76. The table below shows the number of STRs reported by the banking sector.

Table 10: STRs Reported by the Banking Sector

STRs	2023	2024	2025	Total
Money Laundering	2,428	1,822	2,046	**6,296**
Terrorist Financing	1	1	4	**6**
Proliferation financing	-	-	-	**-**
Total	**2,429**	**1,823**	**2,050**	**6,302**

Adequacy of UNSCR Sanctions Screening

3.77. According to Statutory Instrument 76 of 2014 regarding the Suppression of Foreign and International Terrorism (which applies UNSCR 1267 of 1999, UNSCR 1518 of 2003, UNSCR 1988 of 2011, UNSCR 1373 of 2001, and their successor resolutions), as well as Statutory Instrument 110 of 2021 and its amendment, Statutory Instrument 164 (2023) related to the proliferation financing of weapons of mass destruction (which applies UNSCR 1718 concerning Non-State Actor Proliferation in the Democratic People's Republic of Korea) along with its successor resolutions, Statutory Instrument 56 of 2019 (UNSCR 1540 (2004), 1673, 1810, 1887, 1977 (on non-state actor proliferation) UNSCR 1696, UNSCR 1737 (Iran), UNSCR 1747, UNSCR 1803 and UNSCR 1929) together with section 4 of the MLPC Act and AML/CFT Directive No. PFIU3/09/24, banks are required to screen their customers against the UNSCR consolidated list prior to conducting any transactions or entering into any relationships with any individual or entity.

3.78. All banks indicated that they screen their customers against lists of persons and entities issued by the UNSC related to TF and PF. However, onsite examinations noted instances where two (2) banks did not conduct sanctions screening for some of their customers at onboarding.

RESIDUAL RISK

3.79. The residual risk represents the risk that remains after taking into account existing controls. It reflects the net exposure of the banking sector once inherent risk drivers are mitigated by institutional controls, including governance frameworks, internal policies, transaction monitoring systems, customer due diligence (CDD) measures and sanctions screening.

3.80. The sector was rated Medium for money laundering residual risk, driven by Medium-high inherent risk which was moderated by Medium control factors. While inherent exposure remains elevated due to the systemic importance of the sector, concentration of high-risk customers, use of prepaid cards, cross-border activities and branch presence in higher-risk locations, control weaknesses, particularly in transaction monitoring, KYC documentation and governance oversight in some institutions constrained the overall mitigating effect of existing measures.

3.81. Terrorist financing residual risk was assessed as medium-low, reflecting medium-low inherent risk and medium-low control effectiveness. The presence of NPO customers and exposure to certain terrorism high-risk jurisdictions elevated inherent risk. However, this was moderated by the broader national TF risk context and the generally established, albeit variably effective, control frameworks across institutions.

3.82. The rating is also aligned with the National Terrorist Financing Risk Assessment, which assessed Zimbabwe's overall terrorist financing (TF) risk as low, primarily on the basis that the country is exposed mainly to transit-related TF risk rather than significant domestic TF generation or activity.

3.83. Proliferation financing residual risk was rated medium-low, on account of low inherent risk and medium-low control measures. Limited exposure to designated jurisdictions and low trade finance activity reduced inherent vulnerability, although identified weaknesses in monitoring processes, particularly relating to dual-use goods, prevented a lower residual rating.

3.84. For supervisory processes and strategies, the three (3) risk categories were fused together to come up with residual ML/TF/PF risk, based on the weights informed by the NRAs of each category and their perceived threats and vulnerabilities. The conclusion was a rating of medium ML/TF/PF risk on account of medium-high inherent risk and medium control factors, as shown in the table below.

Table 11: Residual Risk

	Money Laundering (ML)	Terrorist Financing (TF)	Proliferation Financing (PF)	ML/TF/PF
Inherent Risk	Medium High	Medium Low	Low	Medium High
Control Factors	Medium	Medium Low	Medium Low	Medium
Residual Risk	Medium	Medium Low	Medium Low	Medium

3.85. Meanwhile, of the sixteen (16) banks, two (2) were rated High risk, one (1) as Medium High risk, five (5) as Medium risk, six (6) as Medium Low risk, and two (2) as Low risk, on a consolidated residual risk rating basis, encompassing money laundering (ML), terrorist financing (TF), and proliferation financing (PF).

3.86. The heat map below summarises the residual risk ratings, thus listing the number of banking institution under each risk category and in accordance with how they were rated.

Table 12: Heat map

HEAT MAP						
Inherent risk	High		1		1	
	Medium High	1		3	1	3
	Medium			2		2
	Medium Low	1		1		
	Low					
		Low	Medium Low	Medium	Medium High	High
		Control Factors				