EFIU HARDWARE DEALERS AML/ CFT GUIDELINE

March 2024

Contents

March 2024

Acronyms

AI - Accountable Institutions

AML/CFT - Anti-money Laundering/ Countering the Financing of Terrorism

CDD - Customer Due Diligence

CRMP - Compliance Risk Management Program

CTR - Cash Transaction Report

DNFBP - Designated Non-Financial Businesses and Professions

EDD - Enhanced Due Diligence

EFIU - Eswatini Financial Intelligence Unit

FSRB - FATF Style Regional Body

INR. - Interpretive Note to Recommendation

ML - Money laundering

MLRO - Money Laundering Reporting Officer

MLCO - Money Laundering Compliance Officer

NRA - National Risk Assessment

PEP - Politically Exposed Person

PF - Proliferation Financing

RBA - Risk-based Approach

SDD - Simplified Due Diligence

SRB - Self-regulatory Body

STR - Suspicious Transaction Report

TF - Terrorist Financing

TCSP - Trusts and company service providers

TPR - Terrorist Property Reporting

1. Section 1: Introduction and key concept

The new section 6 of the MLFTP (amendment) Act, 2016 requires that accountable institution include the application of a risk-based approach to the management of financial crime risk. The risk-based approach requires that anti-money laundering (AML) and the combatting of the financing of terrorism (CFT) requirements, systems, controls, and preventative measures adopted are commensurate to the risks that are being managed. By applying enhanced measures and controls where the financial crime risks are higher, with the option of applying simplified measures where the risks are lower, accountable institutions will be able to target their resources more effectively, whilst ensuring that these risks are efficiently mitigated. Hardware Dealers shall be required to prepare and submit periodically AML/CFT specific risk assessments to the EFIU at least annually or as and when directed.

The application of a risk-based approach also affords accountable institutions flexibility to use a range of mechanisms to establish and verify the identities of their clients, creating opportunities to explore more innovative ways of offering services to a broader range of clients and bringing previously excluded sectors of society into the formal economy. This improves the efficacy of measures to combat money laundering and terrorist financing by deploying limited resources to high-risk areas.

The application of a risk-based approach, as also provided for in Recommendation 1 of the Financial Action Task Force (FATF) and section 6 of the Money Laundering and Financing of Terrorism (Prevention) Act, 2011. It requires accountable institutions to clearly identify, assess and understand and mitigate the financial crime risks that affect their business. Risk in this context refers to the possible threats and vulnerabilities that could lead to accountable institutions' systems, processes or other elements of the business being abused for purposes of ML/FT/PF, specifically including the facilitation of money laundering, terrorism financing, weapons proliferation, and international sanctions circumvention. By understanding the scope and nature of these risks (through risk profiling and risk assessments), accountable institutions can make informed decisions as to the appropriate methods and controls that should be applied in any given circumstance.

Financial crime risk must be assessed on a holistic basis and by means of a systematic approach. This guideline sets out such an approach, together with the risk framework and minimum requirements that accountable institutions should apply when assessing financial crime risk.

Although the risk-based approach aims to manage financial crime risks more efficiently and effectively, it is not possible to eliminate all financial crime risks. It is Important to note that the risk-based

approach does not exempt accountable institutions from mitigating financial crime risks where these risks have been assessed as low.

Furthermore, assessing and mitigating the risk of financial crime is not a static exercise. The risks that have been identified may change or evolve over time as new products or new threats enter the business context.

1.1. Purpose of the guideline

The purpose of this guideline is to provide minimum criteria for the application of a risk-based approach by Hardware Dealers to assist the business in proactively managing financial crime risk by providing for the consistent design, application, and implementation of a risk-based approach. This will further allow for the optimization of resources to ensure that the allocation of such resources is commensurate with the level of risk identified.

1.2. Scope of the guideline

The guideline applies to all Hardware Dealers.

1.3. Ownership and review of guideline

This guideline is owned by the EFIU and shall be reviewed as and when the need arises and especially informed by legislation or industry practices.

1.4. Publication and effective date of guideline

This guidance shall be made available on the EFIU official website on the day of its effective date.

1.5. Risk management concepts

The application of a risk-based approach is based on the following concepts:

a) Risk

Risk can be described as the likelihood and impact of uncertain events on set objectives. The likelihood and impact of such events should be analysed in terms of threats and vulnerabilities.

A threat is a person or group of people, object, or activity with the potential to cause harm. In the context of money laundering and terrorist financing this includes criminals, terrorist groups and their facilitators, their funds, as well as any past, present, and future money laundering, or terrorist financing activities.

The concept of vulnerabilities comprises those things that can be exploited by the threat or that may support or facilitate its activities. Identifying vulnerabilities, as distinct from threats, means focusing on, for example, the factors that represent weaknesses or features that may be exploited in any given system, institution, product, service, etc.
Consequences refers to the impact of a threat or the exploitation of a vulnerability if this impact is to materialize.

Risk in the context of money laundering and terrorist financing therefore refers to the likelihood and impact of money laundering or terrorist financing activities that could materialize because of a combination of threats and vulnerabilities manifesting in the business, or that may jeopardize the detection, investigation or prosecution of these activities or the possibility of the forfeiture of proceeds of unlawful activities.

To have a robust financial crime risk management system, all accountable institutions must be able to demonstrate how they contextualize the concept of "financial crime risk" within their businesses as having an impact on their operational, line management and strategic objectives.

b) Inherent Risk and Residual Risk

Inherent risk is the risk of an event or circumstance that exists before controls or mitigation measures are applied. Residual risk is the level of risk that remains after controls and mitigation measures have been implemented.

c) Risk Management

Financial crime risk management is a process that includes the identification of financial crime risks, the assessment of these risks, and the development of methods and controls to manage and mitigate the risks that have been identified.

Financial crime risk, as with other risks, can be managed and mitigated either by avoiding, transferring, tolerating, or treating different risks. Treating financial crime risk entails that the various franchises, segments, subsidiaries, and international operations must develop systems and controls to manage the risks identified. These systems and controls should comprise of all the risk mitigation measures at the business' disposal and should relate to the nature of risks. Such mechanisms include*, inter alia*:

i. the application of client due diligence measures,

ii. the monitoring of business relationships with clients,

iii. managing delivery channels for products and services,

iv. geographic factors,

v. structuring the features of products and services; etc.

The process to manage financial crime risk is a continuous cycle. Hardware Stores should be satisfied that the financial crime risk management systems and controls remain adequate in view of changing circumstances relating to emerging threats and vulnerabilities, product innovations, new target markets, changes in circumstances of individual clients or classes of clients, changes in business strategy, etc. This means that financial crime risks, controls and the levels of residual risk must be reassessed at regular intervals. The financial crime risk management systems and controls must also be always adhered to.

1.6. Hardware Store's activities and vulnerabilities for ML/TF

The importance of AML/CFT to hardware retail outlets

Albeit not defined as accountable institutions under section 2 of the Act, hardware **stores** are DNFBPs that pose a ML, TF, and PF risks due to the nature of their business operations**.** Recommendation 22 suggests that DNFBPs should be required to comply with the CDD requirements set out in Recommendation 10.

I. Facilitation of money laundering at hardware stores

(a) Customers that are also account holders may deposit funds derived from illegal activities (referred to as 'proceeds of crime') to legitimise the funds. This may be done through simply producing an I.D. that is linked to the account and making a deposit. There are no limits as to the money that can be deposited nor is source of funds required. The is also no limit to the maximum funds that the account can hold at a given time. There are also no daily or monthly transacting limits on the accounts.

(b) Customers may deposit proceeds of crime in the business by using false identity documents or through a third party such as a relative or an unwilling participant recruited by the criminal organisation as a 'money mule'.

(c) Customers may also request refunds from deposited monies at any time through writing to the branch manager and requesting such funds to be deposited into client's given bank account.

By having procedures to more effectively identify Customers and a Program to manage and mitigate ML, TF and PF risk, the AI provides both a deterrent to persons considering the misuse of customers' accounts but also generate records that provide an audit trail that may be relied upon by law enforcement agencies entitled to access the information.

II. Facilitation of terrorism financing at hardware stores

(a) Terrorist organisations derive income from a variety of means, often combining both lawful and unlawful funding sources. The forms of financing are typically grouped into the following categories:

i. financial support – in the form of donations, community solicitation and other fundraising initiatives; or

ii. also, generating activities – income may be derived from criminal activities but also from legitimate economic activities such as real estate and securities investments or generated via normal business activity.

(b) When acting on directions from Customers to transfer funds in accordance with instructions received- such as refunds to a given account, hardware stores need to be aware of circumstances where those funds may be intended for TF activity or are paid in a way it may later be difficult to trace the ultimate destination of those funds. By limiting the way, the hardware stores are permitted to transfer funds and ensuring that the immediate destination of payments by hardware stores are therefore more readily traceable hardware store will be able to better manage and mitigate the risk of misuse of their deposited funds.

An RBA requires Hardware Dealer to mitigate the risks that they face and with due regard to the resources available. Mitigating practices will invariably include initial CDD and ongoing monitoring, as well as a range of internal policies, training, and systems to address the vulnerabilities faced in the operating setting of the Hardware Stores.

As a matter of general principle Hardware Stores who are knowingly engaged in criminal activities do not warrant any special treatment. If they are so engaged, they are criminals and should be treated accordingly. The basic intent behind the FATF Recommendations is consistent with the role of Hardware Stores, to avoid knowingly assisting criminals or facilitating criminal activity. Some of the underlying ethical principles that the Hardware Stores upholds, namely, to avoid facilitating criminal activity and being unwittingly involved in the pursuit of criminal activity, supports the role that Hardware Stores need to play in the fight against ML/TF.

may be especially vulnerable to money laundering due to the increased prevalence of legal entities and vehicles used by corporate buyers and sellers that seek out these properties for investment and revenue. Additionally, the high value of these properties may also require multiple types of financing, which may complicate efforts to identify the source of funds.

2. Section 2: The RBA to AML/CFT

2.1. The guiding principles

Hardware Stores should base their own risk-based assessments and supporting operating standards and procedures on the following guiding principles:

a) It is advised that Hardware Stores adopt and demonstrate a zero tolerance for wilful and deliberate non-compliance with AML legislation and regulations.
b) When applying a risk-based approach, Hardware Stores must comply with all minimum regulatory requirements and all applicable financial crime policies and standards and directives adopted and approved by their boards.
c) Consequences for non-adherence with minimum regulatory and policy requirements should be clearly articulated, specifically for staff members.
d) Each Hardware Store's Financial Crime Risk Management and Compliance Program will comprise of a collection of documents. These various documents should, as far as possible, provide sufficient guidance on a practical level to its targeted audiences.
e) These documents should, where relevant and appropriate, be read in conjunction with any applicable market conduct standards or guidance.
f) Where applicable, definitions should be agreed and applied consistently across the accountable institution.
g) The design of a risk-based approach must be geared towards truly understanding clients and the risk that they represent, supported by robust client due diligence standards and procedures, and must not simply constitute a tick-box exercise.
h) The risk-based approach adopted by the Hardware Store should, as far as possible, be designed to be client friendly and not unnecessarily burden the client.
i) The application of a risk-based approach should support the development and strengthening of a culture of compliance in the Hardware Store's business.
j) The application of a risk-based approach should improve the business' ability to make risk-based decisions.

k) The risk-based approach should enable the use of innovative and cost-effective controls and measures, including the use of new technologies where this is appropriate and effective in managing risk.

l) The risk-based approach should facilitate synergies across franchises, segments, and business units where this is possible and efficient.

m) The risk assessments and franchise risk-based approach documentation must be periodically re-evaluated and updated for it to remain appropriate and current to the risks faced by the business.

2.2. AML/CFT Compliance Officer

AML/CTF Compliance Officer.

(a) An AML/CTF Compliance Officer is someone holding a management position in the Company, and who is responsible for ensuring that the Company complies with its obligations under the Act.

(b) Sec 18 (1) (a) of the Act always requires that DNFBPs have an AML/CTF Compliance Officer appointed for the purpose of overseeing and supervising compliance with the company's AML/CFT Program.

2.2.1 Purpose

AML/CTF Compliance Officer will be responsible for:

(a) maintaining a training program to give all employees appropriate training at appropriate intervals to identify the ML and TF risks that we face.

(b) reporting to the board the suitability of the training program at least once annually.

(c) designing and establishing an employee due diligence program and seeking approval from the board.

(d) providing written reporting to the board and senior management of any detected instances of non-compliance with its AML program.

(e) overseeing transaction monitoring program and conducting, where required, enhanced due diligence checks on existing customers.

(f) disclosing, where required, in reports to EFIU:

i. all Suspicious Transactions.

ii. confirmation of DNFBPs' compliance with the Act applying EFIU standard periodic reporting template.

(g) establishing a procedure to incorporate feedback received from EFIU into the AML Program.

(h) at least annually, obtain an independent review of the AML Program and provide the Board and relevant senior management with a copy of this report.

The AML/CTF Compliance Officer may delegate any of their duties to an appropriately trained and skilled employee as they see fit (also refer 2.1 c) and if appropriate, in the context of the Company's business operations.

2.3. Consequences of non-compliance

2.3.1 Liability of reporting entities-Hardware stores

(a) Breaches of the Act may result in criminal or civil penalties. The penalties for criminal offences include fines of not less than one hundred thousand Emalangeni (E100,000) for body corporates.

(b) Contraventions of the following obligations (CDD, transaction monitoring and STR etc.) may give rise to application of civil penalty orders:

i. providing a service to a customer before carrying out an applicable customer identification procedure.

ii. not carrying out ongoing transaction monitoring and Customer due diligence.

iii. failure to report Suspicious Transactions, Threshold Transactions, or International Fund Transfer Instructions.

iv. providing a service without having adopted an AML Program under the Act.

v. failure to keep records in relation to compliance with the Act including the performance of Customer Identification and Verification Procedures; and

vi. Appoint a compliance officer.

c) In responding to instances of detected non-compliance with the Act, EFIU and responsible regulatory authorities have a broad range of enforcement powers which include undertaking criminal prosecutions, seeking injunctions and civil penalty orders, negotiating enforceable undertakings, and issuing mandatory remedial directions against reporting entities.

2.4. Risk management

It is accepted that Hardware Store cannot be able to completely prevent financial crime. Furthermore, in the application of a risk-based approach, where the Hardware Store is required to focus resources on higher risks situations, there will especially be instances where the Hardware Store is required to accept certain financial crime risks. This may also be required where there is uncertainty of legislative requirements.

ML/TF risk should be managed by transferring, tolerating (accepting), treating, or terminating the risk. An effective financial crime control framework/program requires that the Hardware Store's business clearly articulate, document, and enforce the way it manages its ML/TF risk. This includes setting specific minimum and maximum levels of risk that must be applied when determining whether a risk can be accepted or not. Some of the questions that the Hardware Store may want to answer are:

a) Is the business willing to accept regulatory, reputation, legal or financial risks?
b) What risks is the business willing to accept only after implementing some mitigation measures?
c) What risks is the business not willing to accept?

Accepting risk always requires the application of robust governance procedures, which must include escalation of the risk acceptance for approval to the appropriate governance bodies, which must be at an executive committee level.

2.5. ML/TF/PF risk assessment and risk rating framework

a) A risk-based approach to AML/CFT means that measures taken to reduce ML/TF are proportionate to the risks. Supervisors and SRBs should have a clear understanding of the ML/TF risks present in their own jurisdiction, as well as improve supervisory effectiveness by allocating resources to areas of higher ML/TF risk, in line with the applicable legal framework and the RBA.

b) Importantly the Hardware Store's business must include the way it identifies, assesses, mitigates, and manages the ML/TF/PF risk, this includes the ML/TF/PF risk assessment and risk rating methodology in its CRMP document. The Hardware Store must express and include the inherent ML/TF/PF risk understanding flowing from the ML/TF/PF risk and the risk mitigation, monitoring, and management measures in the CRMP document.

c) This risk-based approach must provide for:

    i. A business level risk assessment indicating the ML/TF/PF risk each of the Hardware Store's different business areas faces.

    ii. The way the Hardware Store's business assesses new products and processes, developed to determine the ML/TF/PF risk ratings or weightings.

    iii. A client level risk assessment indicating the ML/TF/PF risk different types of clients pose.

    iv. Some of the indicators which broadly includes client type, delivery channel, geographic location, products, and services as well as any other relevant factors.

v. The Hardware Stores must stipulate which indicators should be considered when conducting the risk assessments. The Hardware Store is cautioned to consider the holistic indicators.

vi. The Hardware Store must provide evidence that it has conducted client level risk assessments before establishing a business relationship or concluding single transactions with each client.

vii. The Hardware Store must provide evidence of a business level risk assessment, as well as new products and processes assessment.

viii. A risk matrix could serve as a tool to provide an objective basis to the assessment of several risk indicators because the Hardware Store's business risk rates/weights the various indicators characteristics and the method of determining the overall risk ratings/weightings. The method may be either a manual or automated manner of calculating ML/TF/PF risk ratings.

ix. The risk-based approach framework should set out the intervals at which the risk rating will be determined including at the establishment of a new business relationship, before conducting a single transaction and thereafter at predetermined ongoing due diligence intervals.

x. The actual risk rating or weighting assigned to each factor's characteristic should be recorded as part of the methodology and applied uniformly when risk rating.

xi. The way to record the outcome/results of the risk assessments that are conducted. (e.g., when a client establishes a business relationship the outcome risk rating is recorded on the client file).

xii. Hardware Stores can take an informed decision as to the appropriate methods and levels of verification and enhanced controls that must be applied in each circumstance based on risk assessment results.

xiii. The monitoring, mitigating and management controls that must be applied to the different risk ratings must be clearly noted. The steps that must be taken after having assessed the risk must be indicated.

xiv. The CRMP document must provide for the documenting of decisions taken when dealing with the different levels of ML/TF/PF risk that result.

xv. Hardware Dealers should conduct ML/FT/PF risk assessments and share with the EFIU at least annually.

2.6. Application of the risk-based approach

The application of a risk-based approach consists of the following distinct steps:

a) Identification and assessment of inherent risk.
b) Creating risk-reduction measures and controls.
c) Assessing residual risks.
d) Evaluating residual risk against set business unit risk appetite; and
e) Reviewing the risk-based approach.

Each of these requirements is discussed in more detail below.

2.7. Identification and assessment of inherent risks

In terms of the new section 6 above, accountable institutions must complete regular financial crime risk assessments. Through these assessments, accountable institutions should identify the financial crime risks they may face in the context of their business and analyse these with a view to understand the likelihood of the risk materializing and the impact that this would have.

The mechanisms used by the Hardware Store's businesses to identify and assess their financial crime risks must be proportionate to their size and complexity. The risk assessment process therefore might be quite simple or very sophisticated depending on the size and structure of the business and the nature and range of products and services it offers. These risk assessments must form the basis of the risk-based approach that is adopted by the Hardware Store's business.

Factors that may be indicative of financial crime risks relate to several aspects, including:

a) product offered,
b) service features associated to products or as stand-alone service,
c) delivery channels,
d) geographic areas; and
e) the client risk profile of the business' client base.

Each of these may interact differently with the characteristics of different types of clients.

The examples of factors that may be indicative of financial crime risk provided in **Annexure 1** are not an exhaustive list and Hardware Store must therefore also consider other factors that may be relevant

to their own businesses. Furthermore, the examples provided here are phrased in neutral terms – i.e., a factor may be indicative of either higher or lower risk depending on the context within which it is considered. It is important therefore to demonstrate how different indicators are brought to bear on a given scenario to reach an appropriate risk classification.

A business risk assessment could utilize a combination of internal subject matter experts; the business risk function; available publications; and external advice. It could also incorporate any future initiatives, previously reported financial crime incidents or events, issues and control failures identified by the respective assurance functions. The assessment must be dynamic and responsive to current and emerging risks.

To be effective, the risk assessment must be properly documented, maintained, and communicated to relevant personnel within the business. A detailed and well documented compliance regime shows commitment to prevent, detect and address non-compliance within the business.

2.8. Creating risk- reduction measures and controls

Risk mitigation in the context of financial crime refers to the activities and methods used by the Hardware Store's business to control and minimize the inherent financial crime risks it has identified. The Hardware Store's business should therefore apply its knowledge and understanding of its financial crime risks, as assessed per the guidance above, in the development of control measures to mitigate the risks identified. The risk assessment process will therefore assist the Hardware Store's business in determining the nature and extent of resources necessary to mitigate identified risks.

Each business unit or segment of the Hardware Store's business must establish and implement systems and controls in response to the assessed risks. These controls must be designed to detect money laundering and terrorist financing and respond appropriately when risks materialize. Where the risks are higher, enhanced measures must be taken to mitigate those risks. This means that the range, degree, frequency or intensity of preventive measures and controls conducted will be stronger in higher risk scenarios. Where the risks have been assessed as lower, simplified measures may be permitted, such as that the degree, frequency and/or the intensity of the controls conducted may be relatively lighter. Hardware Stores should always have grounds on which they can base their justification for a decision that the appropriate balance was struck in any given circumstance.

The following are some measures that may be applied in cases of higher risk:

a) Increased automated transaction monitoring,

b) increased intensity of CDD measures,

c) increased review periods of client information,

d) utilizing more or higher quality sources for the vetting of information (impacts both quality and quantity),

e) senior management involvement in decisions to on-board clients,

f) dedicated specialist staff managing enhanced due diligence for specific clients; and

g) limited reliance on another accountable institution's controls, together with additional controls.

It is important to note that the risk-based approach requires the business segments of the Hardware Stores to adopt effective AML/CFT controls that are commensurate to their assessed risks. It is the responsibility of the business unit to effectively manage all financial crime risks and to meet all applicable minimum legal requirements as the first line of defense.

The systems and controls by which the business decides to manage financial crime risks must be documented in the applicable and relevant accountable institution's processes and procedures.

2.9. Assessing residual risks

Residual risk is the risk remaining after taking into consideration the impact and effectiveness of risk mitigation measures and controls. It is important to note that no matter how robust the risk mitigation and risk management program is, the business may always have some exposure to residual risk which must be managed. These risks have been reduced but not eliminated and are therefore still risks.

2.10. Evaluating residual risk against set risk appetite

Finally, it must be assessed whether the residual risk that has been identified falls within the set risk appetite of the business. Where the level of residual risk falls outside of the scope of acceptable risk, additional controls and measures must be adopted to mitigate the risk further.

2.11. Reviewing the risk- based approach

The risk-based approach implemented by the Hardware Store's business should be subject to periodic review, as required in terms of paragraph 6 above which is to the effect that Hardware Stores are carrying out the activities under recommendation 22 above are accountable institutions and shall update their risk assessment policies and programs regularly but at least annually considering new

markets and introduction of new products and services, to test the effectiveness of the compliance regime. This review includes but is not limited to:

a) applicable policies and procedures
b) the risk assessment related to financial crime, including the adequacy of controls and other risk mitigation measures; and
c) the training program used for employees and senior management.

The risks that have been identified will change or evolve over time as new products or new threats enter the business context. Consequently, the adherence and completion of this step is crucial to the implementation of an effective risk-based approach.

2.12. Clients risk profiling requirements

a) Clients risk assessments

A Hardware Store's business' AML/CFT Program and policy must require that all clients be risk assessed at the time of on-boarding, or as soon as possible thereafter, and for the duration of the client relationship life cycle on an on-going basis. This initial risk rating therefore represents the inherent risk posed by the client (prior to transactional behaviour commencing) and it is important for purposes of *inter alia* applying the appropriate level of due diligence during the on-boarding process.

A client, for purposes of this guideline, is a natural person or corporate vehicle with whom the legal professional's business has established a business relationship as listed under recommendation 22 above. A business relationship is created at the point at which the client is enabled by the business to transact, deposit, receive funds or accept products or services offered by the Hardware Store's business.

Risk-rating implies assigning different categories to different levels of risk per a risk scale and classifying the financial crime risks pertaining to different relationships or client engagements in terms of the assigned categories.

The on-going risk assessment of clients comprises of at least two types of risk assessments:

b) Initial risk assessment

A risk-based approach commences with the assessment of risk that needs to be managed, i.e., the initial risk assessment. This should, where possible, be performed at the time of client on-boarding.

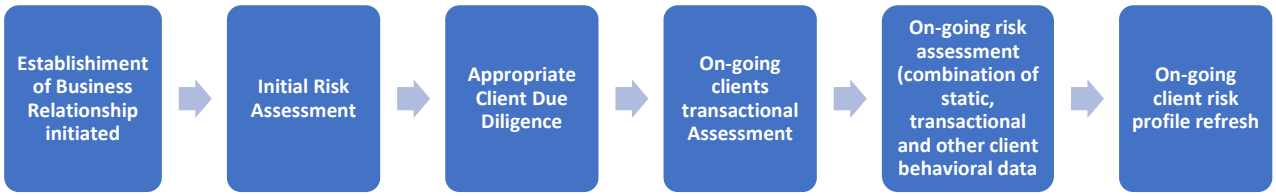
Alternatively, the initial risk assessment must be completed as soon as possible once a business relationship has been established.

The initial risk assessment should at a minimum incorporate all relevant and available static client data obtained through the application of the required client due diligence measures.

c) On-going comprehensive risks assessments

While a risk assessment should be performed at the inception of the client relationship, a comprehensive risk profile of the client will only become evident once the client has begun transacting through an account or begins utilizing a service or product. The monitoring of transactions; other client behaviour; and the business relationship are therefore important elements of a well-designed risk-based approach. Once a client has been risk rated, this rating must therefore be continuously re-assessed for the duration of the client relationship life cycle. This risk assessment process flow is illustrated below:

Figure 1: Risk assessment process flow



The on-going comprehensive risk assessment models should, in addition to the static factors used for the initial client risk assessment, and to the extent possible, include a dynamic component incorporating the transactional or other behaviour of the client into their risk rating. Once the client starts transacting (where this is applicable), the initial risk assessment may therefore change due to the nature of transactional behaviour of the client or other subsequent factors which may emerge. A lower risk client may thus become higher risk, or alternatively, a higher risk client may become lower risk, based on considerations of both the client static data and transactional behaviour, providing a consolidated and true view of risk of the client relationship.

Where possible, this process is to be embedded as an on-going process and not performed as a calendar driven event.

2.13. Risk model

Both the initial client risk assessment models and the on-going comprehensive risk assessment models for individuals and entities must be determined by each business segment, based on the risk criteria contained in each Hardware Store's Financial Crime Policy and this guidance, as well as any factors unique to that Hardware Store's business.

Such models must enable effective and appropriate client risk categorization, considering the money laundering and terrorist financing risk to each hardware store's business across its clients; the industries and jurisdictions in which they operate; products offered; delivery channels utilized; and the on-going transactional behaviour of its clients. The ultimate risk rating must be the result of a holistic consideration of these factors.

The following risk factors / variables that, either on their own or in combination, may increase or decrease risk, should be considered when determining the risk rating of a client, unless reasons can be provided showing that a factor is not relevant to a specific risk model in the context of the business in which it will be used:

Table 1: Inherent Client Risk

Static Variables	
Inherent Client Risk	An assessment of the inherent risk of the client, including factors such as the residency status of a client; the nature and frequency of transactions; the legal status of the client (natural person or corporate vehicle) or the entity type or structure through which the client operates. Inherent client risk can also include factors such as whether the client has been linked to adverse media relating to financial crime.

Table 2: Static Variables

Static Variables	
Products & services offered	An assessment of the financial crime risk posed by the products and/or services utilized by the client. It is important to note that criminals constantly alter their methods and techniques and therefore the assessment of products and services must be dynamic.
	An assessment of the jurisdictions within which the business operates as well as assessment of where clients live and work.

Geography	
Client industry (Including business activity)	An assessment of the industry the client works in or, in the case of a business or corporate, the nature of the business. Certain industries are more closely associated with money laundering or terrorist financing risks, as determined by FATF from time to time. Cognizance should also be taken of whether the industry is regulated in the jurisdiction within which it operates.
Distribution channel (which can be assessed as part of product risk)	The method of distributing products and services at point of account opening as well as on an on-going basis.

Table 3: Dynamic Variables

Dynamic Variables	
Transactional behaviour	Where applicable, once the client starts transacting, financial crime risk must be assessed based on the client's transactional behaviour. Aggregated transactional risk assessment models for transaction types (e.g., debit card transactions; credit card transactions; electronic funds transfers; and SWIFT transactions) may be used to assess client risk in conjunction with the criteria reflected above.
Other behavioural factors	Where applicable, any other behavioural factors relevant to an assessment of the client's expected behaviour vs. their actual behaviour, and which indicates risk, should be included in the risk model.

It is imperative that the money laundering risk in any given circumstance be determined on a holistic basis. In other words, the ultimate risk rating accorded to a business relationship or transaction must be a function of all factors that may be relevant to the combination of a client profile, product type and transaction.

The aggregated model should be combined with the initial risk assessment to provide a view of the ongoing risk the client poses to the business. This is illustrated in the diagram below:

Table 4: Risk assessment Diagram

Risk Assessment Diagram					
Risk Assessment	**Initial Risk Assessment *(Analytical Modelling)***	+	**Transactional Risk Assessment *(Analytical Modelling)***	=	**On-going consolidated Risk Assessment *(Analytical Modelling)***
	⬇		⬇		⬇
Controls	**Level of Client Due Diligence** • **Simplified due diligence.** • **Standard due diligence.** • **Enhanced due diligence.**		**Transaction Monitoring** • **Suspicious transactions monitoring** • **Cash Threshold monitoring** • **Scenario monitoring** • **Terrorist property monitoring**		**Client Refresh Cycle** • **Enhanced due diligence (*Annual Refresh)*** • **Standard due diligence (*Refresh every 3 years or at trigger event*)** • **Simplified due diligence (*Refresh every 5 years or at trigger event*)**

The risk-rating methodology and procedures that have been adopted for purposes of client risk rating must be properly documented and are subject to approval by each hardware store's board (where applicable). It must furthermore record the basis for allocating risk categories to individual and aggregate risks and the rationale for setting controls against specific risks, including the rationale for the configuration of the financial crime automated systems and risk models.

The factors underlying any given risk-rating will furthermore inevitably change over time. It is therefore essential that the relevance of particular risk factors and the appropriateness of previous risk-ratings be re- assessed on a periodic basis, or when changes to the business, legislative or regulatory environment require such updates.

2.14. Automatically high-risk clients

All clients that are deemed to be high risk in accordance with applicable domestic legislation must be risk rated as high, irrespective of any of the other factors in the applicable risk assessment model.

The following client relationships, when evident, will also result in the overall client relationship becoming high risk, irrespective of any of the other factors in the risk assessment model:

a) Politically Exposed Person as defined in section 2 of the Money Laundering and Financing of Terrorism (Prevention) Act,2011 (MLFTP) 2011 (as amended)
b) Persons identified as "Persons of Interest" through internal governance structures, and who have been included on the internal business watch lists or exit lists.
c) Money service businesses (MSBs).
d) Virtual currency providers and exchanges.
e) High commissions and embassies of high-risk jurisdictions, as per the business' Risk Matrix
f) Foreign charities and foreign trusts.
g) Arms dealers.
h) Correspondent banking (Vostro accounts).
i) Second-hand gold and scrap metal dealers; and
j) Trade, dealing in or breeding endangered or protected species.

The categories of automatically high-risk clients will be reviewed and updated from time to time by each accountable institution, as the need arises.

Automatically high-risk clients may be reclassified post the completion of EDD. However, where it is a regulatory requirement that a client automatically be deemed to be high risk – as is the case with PEPs. Reclassification is prohibited.

2.15. Impact of client risk rating

The client risk rating should inform and determine the processes and controls applicable to that client, or class of clients, which are proportionate to the level of money laundering and terrorism financing risk presented by each client relationship. These processes include, but is not limited to:

a) the appropriate level of client due diligence (CDD) that must be conducted.
b) the appropriate level of management approval / acceptance required to establish or continue with a business relationship.
c) the appropriate level of monitoring (transactions and activities); and
d) the appropriate level and frequency of on-going due diligence (ODD) to be applied.

The processes and controls relating to client due diligence will be set out in further detail in each accountable institution's Client Due Diligence Minimum Operating Standard.

2.16. De-risking

It is important to note that risk assessment does not imply that the hardware store's business should seek to avoid risk entirely (also referred to as de-risking), for example, through wholesale termination of client relationships for certain sectors. De-risking poses a threat to financial integrity in general and to the risk-based approach specifically, as it creates opacity in the affected persons' or entities' financial conduct, and it eliminates the possibility to treat financial crime risks. Wholesale refusal of services or termination of services to a class of clients may further give rise to financial exclusion risk and consequently also reputational risk to accountable institutions.

The wholesale termination or restriction of business relationships should therefore, where possible, be avoided as this is an example of inadequate risk management.

2.17. Financial crime risk management

a) Hardware Store's in their effort to implement an effective Financial Crime Risk Management (FCRM) will develop the client static and transactional risk models as well as the overall risk model which considers both initial and transactional risk as a combined risk.

b) A Hardware Store's business' (conducting any of the activities under recommendation 22 above) FCRM shall be responsible for documenting the detailed business systems and model configurations and ensuring that these are approved by the Boards or other relevant governance forum. The rationale for the adoption of such system and model configurations, as well as the

implementation of the controls must be recorded and monitored by FCRM function of the Hardware Store's business.

2.18. Compliance risk management program (CRMP)

Hardware Stores must develop, document, maintain and implement a CRMP for anti-money laundering, combating the financing of terrorism and counter proliferation financing (AML/CTF/CPF), which programme is referred to as the DNFBPs CRMP. The CRMP must provide for all the requirements as set out in section 18 of the MLFTP Act, UNSCR (2016) and Suppression of Terrorism Act, 2008.

a) Hardware Stores must have a main consolidated document or overarching apex document that records the CRMP, which document is referred to as the CRMP.

b) Hardware Stores must express and include the inherent money laundering, terrorist financing and proliferation financing (ML/TF/PF) risk, and its understanding flowing from the ML/TF/PF risk assessments, and the risk mitigation, monitoring as well as the management measures in the CRMP.

3. Section 3: Customer due diligence

3.1. CDD introduction

In terms of the Kingdom of Eswatini (hereinafter referred to as "Eswatini") regulatory requirements, particularly the Money Laundering and Financing of Terrorism (Prevention) Act 2011 as amended by the Money Laundering and Financing of Terrorism (Prevention) Act No. 05 of 2016, (hereinafter referred to as "ML / TF" (P) Act, 2011 as amended) DNFBPs which Hardware Stores are a part of may not establish a business relationship or conclude a single transaction with a customer unless the required standard of customer due diligence has been undertaken and completed.

In terms of S31 (1) (I) the EFIU has formulated a Customer Due Diligence/ Know Your Customer guideline, referred herein as "the guideline", based on the criteria/ guidelines specified in "ML / TF" (P) Act, 2011 (as amended) and FAFT recommendations respectively. S31 (1) (I) provides that the EFIU "**shall issue guidelines to accountable institutions not under the jurisdiction of supervisory authorities in relation to customer identification, record keeping and reporting obligations and the identification of suspicious transactions."**

This guideline defines different types of customers, their minimum required information, and documents along with the characteristics of High-Risk Customers, who pose greater than average risk of money laundering activities and terrorist financing. It further explains how to ensure the identity of the clients, who initiate relationship with the Hardware Store and how to maintain and update the CDD/KYC measures for existing customers/clients. It further outlines the training to be given to officers, employees (inclusive of the Board where applicable), and as well as compliance with the regulatory requirement of record retention/keeping.

a) Scope

This guideline outlines the minimum requirements to be followed by all Hardware Stores and their employees, agents, secondees and contractors (contingent workers) that engage with customers when executing elements of the business relationship life cycle defined in 2.2 below. These apply to.

i. All prospective customers that intend to establish a business relationship with and/ or conduct a single transaction.
ii. Existing customers that intend to continue a business relationship with and/ or conduct a single transaction.

Some Hardware stores may accordingly be able to conclude that based on the services they provide, they do not have any specific AML/CFT obligations as they do not prepare for or carry out any of the specified activities. Even though specific AML/CFT obligations may not apply to a Hardware Store, it is consistent with the overall ethics and best practices of the profession for all hardware stores to ensure that their services are not being misused, including by criminals. Accordingly, Hardware stores should carefully consider what they need to do to guard against that risk irrespective of the application of specific AML/CFT obligations in order not to be unwittingly involved in ML/TF.

3.2. Purpose of CDD guideline

The purpose of this Guidance is to:

a) Assist all Hardware Stores in the design and implementation of an RBA to AML/CFT compliance by providing guidelines and examples of current practice, with a particular focus on providing guidance to sole practitioners and small firms.

b) Support a common understanding of an RBA for Hardware Stores, that maintain relationships with Hardware Stores and competent authorities and self-regulatory bodies (SRBs) responsible for monitoring the compliance of Hardware Stores with their AML/CFT obligations,

c) Outline the key elements involved in applying an RBA to AML/CFT applicable to Hardware Store.

3.3. Types of customers, information and documents required:

Hardware Stores engaging in the above AML/CFT related instructions shall obtain the minimum information or set of documents from various types of customers for account opening purposes, detail of which are as follows:

Table 5: Customer Types and KYC Requirements

Customer Type	Information Required	Documents Required

Individuals / Sole proprietorship	• Full Name
	• Physical Address
	• Telephone Number (s)
		• **National Identity Document**
		  ○ National ID for Swazis
		  ○ Passport for non-Swazis
		• **Proof of Residence** (For both Individuals and Sole Proprietorship)
		• **Source of Income** (*For both Individuals and Sole Proprietorship*)
		• **Proof of Employment Income** (*For both Individuals)*
		• **Details of Business** (*For Sole Proprietorship*)

Companies (Institutions and Corporates)	• Name of Company and its Directors • Company Registered Physical Address • Company Registration Number • Company Contact Person (Name and contact number)	• **National Identity documents for Company Directors** (*National ID for Swazi Directors and Passports for Non-Swazi Directors*) • **Memorandum and Articles of Associations** • **Certificate of Incorporation** • **Board Resolutions authorizing the investment / engagement.**
Clubs, Societies and Associations	• Name of Club, Society and Association • Registered address of Club, Society and Association • Company Contact Person (Name and contact number)	Certified copies of Club, Society or Association Chairman and signatories By laws or constitutions or rules or regulations of the club or Society or Association.

3.4. Principles of CDD / KYC

Hardware Stores should abide by the following principles for the effective implementation of their KYC policies. These principles shall be applicable to all existing and new customers or clients, details of which are as follows.

a) Deposits or payments in cash require the establishment of sources of funds.

b) CDD/ KYC measures shall be enhanced for High-Risk Customers. Characteristics of high-risk customers are given in 3.7 below.

c) Dealing with any Political Exposed Person or customers holding public or high- profile position, relationship with them should be established and/ or maintained with the approval of Senior Partners including if any existing customer becomes holder of any public office or high-profile position.

d) For customers that are legal persons or for legal arrangements, it is required to take reasonable measures to understand.

    i. the ownership and control structure of the company.

    ii. determine who owns or controls the company (ultimate beneficial owner). This includes those persons who exercise ultimate effective control over a company.

e) In case Hardware Stores are not able to satisfactorily complete the required CDD/ KYC measures, account should not be opened, business relationship should not be established, and business transaction should not be carried out. Instead, reporting of suspicious transaction is considered. Similarly, relationship with existing customer should be terminated, and reporting of suspicious transactions be considered if CDD/ KYC is found unsatisfactory.

3.5. CDD verification

a) Verification is an integral part of CDD/ KYC measures for which Hardware Stores are required to ensure the following areas.

b) Before opening an account, Hardware Store shall verify the copy of ID by asking customer to provide same along with original ID or certified copy thereof. Further thereto, external sources shall be used by Hardware Stores to verify all KYC documents submitted by its clients.

3.6. Beneficial Ownership

In the act a "beneficial owner" is defined as a person or persons who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted and includes those persons who exercise effective control over a legal person or arrangement.

a) It is a requirement that as a Specified Party you establish and verify the identity of the customer, beneficial owner or beneficiary of life insurance and other related investment services.

b) You are further required to obtain information on the occupation of beneficial owner and the source of wealth/funds of a beneficial owner.

c) Beneficial owner can only be a natural person, i.e., an individual (other than in the case of a trust).
d) A hardware, in accordance with their legal obligations, need to be diligent in their enquiries about beneficial ownership, considering that the information they need may not always be readily available from public sources.
e) A flexible approach to information gathering will be needed as it will often involve direct enquiries with clients and their advisers as well as searches of public records in Eswatini and overseas.

There may be situations in which someone is the beneficial owner by virtue of control even though their ownership share is less than the set standard.

3.7. Record updates and retention (on-going due diligence)

a) As part of a risk-based approach, CDD/ KYC should not be contemplated as a once off exercise undertaken at the time of entering a relationship with customers. It should be viewed as an ongoing process and should encompass the following.

b) Maintain proper records of customer identifications and clearly indicate in writing any exception in fulfilling CDD/ KYC measures. These exceptions will be referred to senior management, Board (where applicable) to decide future course of action.

c) Furthermore, Hardware Stores shall keep records regarding the identification data obtained through the customer due diligence process (e.g., copies or records of official identification documents, proof of residence, similar documents) account files and business correspondence for at least 5 (five) years after the business relationship is ended or more in terms of the Act (as amended).

3.8. Customer risk profiling (high risk customers and low risk customers)

a) Hardware Stores are required to conduct enhanced customer due diligence if the customer(s) falls within the definition of High-Risk Customers, which are defined as.
    i. Non-resident customers
    ii. Non-legal persons or arrangements including non-governmental organizations (NGOs) / Not for profit organizations (NPOs) and Trusts/ charitable organizations.
    iii. High net worth customers with no clearly identifiable source of income.

iv. Customers dealing in high value items.

v. Politically Exposed Persons (PEPs). Those individuals who are or who have been entrusted with prominent public functions in a country or territory, for example heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned entities, important political party officials but not middle ranking or more junior individuals in these categories.

vi. Customers from or in countries where CDD/ KYC and anti-money laundering Regulations are lax and are not sufficiently applying Financial Action Task Force (FATF) Recommendations.

vii. Customers who have been refused by another financial institution (based on reasonable information).

viii. Clients subject to adverse media are high profile individuals who may be potentially linked to adverse or negative news.

b) Sanctioned Entities-If the customer is listed as a sanctioned entity/person, no business relationship should be established. In the event the same had been already established, same should be exited forthwith by following the laid down procedure.

c) For low-risk Customers, a simplified or reduced CDD/ KYC measures will be applied. A client may be considered under low-risk category if the identity of the customer(s) and the beneficial owner of a customer are publicly known or where adequate checks and controls exist.

d) The following case(s) may inter alia be considered as low-risk Customers for application of simplified or reduced CDD/ KYC.

ix. Financial institutions provided they are subject to requirements to combat money laundering and terrorist financing and are supervised for compliance with those requirements.

3.9. Customer due diligence controls

Hardware Stores must include in the apex CRMP document its customer due diligence (CDD) procedure, which should indicate the way the Hardware Store's business:

a) Determines which persons are deemed to be clients, and further determine whether a person(s) is an existing client.

b) Prevents the on-boarding of anonymous clients, and clients acting under a false or fictitious name.
c) Conducts CDD on the different types of potential clients, existing clients, beneficial owners, persons acting on behalf of the client and other persons. This includes determining the level of verification which forms part of the CDD because of the client's risk rating.
d) Conducts Additional due diligence (ADD) in respect of clients that are legal persons, trusts, or partnerships.
e) Conducts ongoing due diligence (ODD) and at which intervals.
f) Conducts enhanced due diligence (EDD) where a high-risk business relationship has been identified.
g) Conducts simplified due diligence where a low-risk business relationship has been identified.
h) Conducts client on-boarding approval including for high-risk business relationships.
i) Determines processes where CDD cannot be conducted.
j) Conducts client profiling including determining which future transactions are consistent with the institution knowledge of a prospective client.
k) Confirms whether information relating to a client, where the DNFBPs doubts the accuracy of previously obtained information.
l) May conduct CDD where there is a suspicion regarding an activity or transaction.

3.10. Customer exit

a) Hardware Stores must implement procedures and processes to manage the exit of customer relationships where they are prohibited or present an unacceptable financial crime risk. This must include the requirement to:
    i. Assess the customer relationship and document.
    ii. The financial crime risks posed by the customer with reference to the AML/ CFT risk appetite and any contractual conditions, regulatory expectations and, where applicable, competition law, that must be considered in deciding whether to retain or exit the customer relationship as well as the rationale for the decision to exit the customer relationship.
    iii. Specify a plan and timeline for exiting the customer relationship in line with the existing forum established for this purpose.

3.11. Employee Due Diligence

Section 18(1)(b)(vi) of the Act requires that Accountable Institutions (AI) carry out Employee due diligence (EDD). EDD is carried out by performing checks during the recruitment phase for new Employees, and on an ongoing basis for continuing Employees. The purpose of Employee due diligence is to reduce the risk of Employees being involved in the facilitation of ML or TF activity in connection with the provision of the AI's Services or products. The human resources manager (HRM) (with the oversight of the AML/CTF Compliance Officer) is responsible for establishing and maintaining the Employee due diligence in accordance with AI's AML Program.

a) Employee Due Diligence Process – New Employees

   If the (HRM) assigns a medium to high risk to the role, AI must obtain prior to making any offer of employment to the person, and as far as practicable to obtain, the following information in relation to the person:

   i. the results of at least one, and where possible two, reference checks from previous employers of the person.

   ii. at least one-character reference from a non-family member who has known the applicant for a period of at least two years.

   iii. A police clearance record (where applicable)

b) If the searches or reference checks are unable to be obtained or reveal any adverse or seriously inconsistent results, the AML/CFT Compliance Officer and human resources department will meet to consider whether it is appropriate to employ the person. A record of all searches conducted and any discussions in relation to a decision to employ must be recorded and maintained in accordance with the record keeping obligations set out in section 10 of this guideline.

c) Employee Due Diligence Process - Existing Employees

   i) If an Employee is offered a promotion or is offered a role which increases their level of responsibility or autonomy, the human resources department must give the employee a description of the role.

   ii) Having regard to the Company's ML/TF risks, the HRM must assign the proposed role a risk rating, having regard to whether the role would be reasonably likely to allow the person a significant opportunity to facilitate ML or TF activity.

iii) If the HRM assigns a high risk to the role, the HRM must ensure to obtain, to the extent that they have not earlier been obtained in relation to the Employee, the results of the same checks as set out in paragraph 5.2(b) above.

iv) If these checks reveal any adverse or seriously inconsistent results, the AML/CFT Compliance Officer and human resources department will meet to consider whether it is appropriate to promote the applicant. A record of all searches conducted and any discussions in relation to a decision to employ must be recorded and maintained in accordance with the record keeping obligations set out in section 10 of this guideline.

3.12. Training

a) The training plan which is owned by each Hardware Store's business as an accountable institution, and it is the responsibility of the Anti-money Laundering Compliance Officer to ensure that the training plan consists of general awareness Anti-Money Laundering and role-based trainings. The learning plan applies to all employees including part time employees and contractors/contingent workers, (collectively referred to as employees).

b) All employees are required to complete the training at least twice on an annual basis. Once at onboarding and one refresher. It is required of existing employees that once a new training module has rolled out, the training to be completed within the prescribed timelines. It is also possible that specific training modules be developed for specific target population and business areas and need to be completed in the required timelines- role based trainings.

c) Hardware Stores are further responsible for creating and developing a training plan for its officers, employees, and agents/brokers relating to suspicious transactions, trends in money laundering and financing of terrorism risks in its specific jurisdictional area. The training provided should be aligned to the local law and regulations. Awareness should be created amongst all employees regarding this training which should similarly be completed by all employees at least twice annually as explained above.

d) It is noted that the relevant supervisory authorities are required to facilitate training, under its supervision, for accountable institutions. The training to be facilitated by the supervisory authority will be determined through a series of inspections conducted. It is imperative that Hardware Store similarly create awareness amongst all employees regarding this training and ensures that it is completed as and when required by the relevant supervisory authority.

3.13. Reporting

a) To prevent any unlawful activities and/or inadvertent participation therein, it is pertinent that transactions are monitored to identify any suspicious transactions which relate to anti- money laundering and financing of terrorism. Where reasonable grounds exist of a suspicious transaction this must be reported in terms of the prescribed reporting mechanism and within the duly prescribed time periods i.e., within two working days.

4. Section 4: Politically exposed persons

4.1. Introduction

Politically Exposed Persons" (PEPs) can be defined as individuals (or close family members and those closely associated with these individuals) who are or have in the past been entrusted with prominent public functions in a particular country.

Due to their power and influence, many PEPs are in positions that can potentially be abused for the purpose of committing corruption, bribery, and money laundering offences, as well as conducting activity related to terrorist financing.

Because of the additional risk therefore posed by such individuals, PEPs are a special category of clients, designated as representing higher risk to the Hardware Store's business. The potential risks associated with PEPs furthermore justify the application of additional financial crime controls.

4.2. Purpose of PEP guideline

a) This guideline is aimed at better enabling Hardware Stores in complying with the relevant regulatory obligations relating to financial crime and PEPs, and to protect their practices/businesses from reputational and regulatory damage arising from non-compliance.
b) The purpose of this guideline is to provide necessary guidance on the requirements relating to onboarding PEPs for business purposes and the measures required to mitigate and manage any risks posed by such individuals.

4.3. Politically exposed persons documentation

Hardware Stores must document their processes regarding Politically Exposed Persons in the CRMP document which sets out:

a) The way to scrutinise prospective clients, persons acting on behalf of the client and beneficial owner's information to determine whether they are domestic PEPs, their immediate family members or known close associates.

b) The way the Hardware Store will obtain senior management approval to establish a business relationship with a Foreign PEP & local PEP.

c) The data sources relied upon to determine whether a client is a PEP.

4.4. PEP categorization

In terms of this guideline, and in accordance with FATF Recommendation 12, and the Money Laundering and Terrorist Financing (Prevention) Act 2011, as amended, PEPs have been categorized as follows:

a) A Head of State or Government- King, Prime Minister, Deputy Prime Minister, and all cabinet Ministers.
b) A politician on the national level- All members of the house of Senate and House of Assembly, Consular, Ambassadors.
c) A senior Government official: Undersecretary, Private secretary, Chiefs, Tindvuna.
d) Judiciary- The country's judicial members including all Judges and Magistrates.
e) Military Official-Head of Royal Eswatini police, Eswatini Umbutfo Defence Force, His Majesty's Correctional services, Fire, and emergency services.
f) A senior executive of a State-owned enterprise.
g) An individual or undertaking identified as having.
    i. close family ties or personal or business connections to any of the persons.
    ii. Immediate Family Members due to their proximity to the person entrusted with the prominent public office, the associated PEP may be able to abuse the position of a family member to undertake illicit activities.
h) To this section, an immediate family member includes –
    i. the spouse, civil partner, or life partner.
    ii. the previous spouse, civil partner, or life partner, if applicable
    iii. children and stepchildren and their spouse, adopted children and their adoptive parents, civil partner, or life partner.
    iv. parents; and siblings and step siblings and their spouse, civil partner or life partner and known close associates. Known close associates should be similarly categorized and subjected to the same requirements set out in this guideline, as applicable.

The category of "closely associated persons" typically includes close business colleagues and personal advisers / consultants to the PEP, as well as persons who obviously benefit significantly

from being close to such a person. Close associates can therefore be individuals who are closely connected to a PEP, either socially or professionally. Due to their proximity to the person entrusted with the prominent public office, the PEP may be able to abuse the position of an associate to undertake illicit activities.

4.5. PEP Identification

PEP identification can occur in multiple ways. Business areas dealing with clients should utilize available and appropriate tools, techniques, systems, and strategies to:

a) identify PEPs before the establishment of a relationship with a prospective client.
b) identify existing clients who are, or who have subsequently become; and
c) identify prospective or existing clients that are immediate family members or known close associates of PEPs, or of individuals who have subsequently become PEPs.

For the purposes of this guideline 'PEP' refers collectively to both foreign and domestic PEPs, immediate family members or known close associates of those PEPs, unless specifically stated otherwise.

5. Section 5: AML/CFT internal controls

5.1. Internal control's introduction

Hardware Stores must adopt appropriate controls regarding the size and the nature of the business. There is no standard solution to the design of internal control systems, and this should be considered when Hardware stores are devising an AML/CFT framework. Internal controls will also depend on the business structure, size, and internal organisation without prejudice to the effectiveness of the system. Policies, procedures, and control systems must be designed and implemented with a view to ensuring the ML/TF risks are promptly identified and mitigated in line with the RBA. Internal control systems must be evaluated to determine how effectively they are dealing with the overall risks. Risk-based processes must be established within the internal controls of the businesses to be effective. To be successful, internal policies and procedures are largely dependent on the internal control systems.

5.2. The internal controls for Hardware Dealers

Hardware Stores' businesses should:

a) Have an adequate and effective AML/CFT compliance function with a process in place for a regular review of the policies at appropriate levels. The appointment of a Compliance Officer is fundamental in the implementation of AML/CFT compliance framework.
b) Implement risk based CDD and procedures.
c) Ensure that adequate controls for high-risk customers, transactions, and products, including the launch of new products and services.
d) Focus more resources on the operations of the business that are perceived to be a higher risk to ML/TF
e) Conduct periodic AML/CFT risk assessments and regularly review the risk assessments, considering geographic, customer, delivery channel, and products/ services risk factors.
f) Contain a detailed documented suite of AML /CFT policies and procedures that accurately reflect the operational practices of the business and demonstrate compliance with all legal and regulatory requirements that may also be supplemented and supported by guidance from supervisors or other competent authorities.
g) Have AML/ CFT policies and procedures that are accessible and fully implemented and adhered to by all staff which are regularly reviewed, updated, and approved by Top Management or the board.
h) Enable the timely identification of reportable transactions and ensure accurate filing of required reports. These may be suspicious transactions reports, cash threshold reports, responses to Supervisors and other competent authorities' requests.
i) Ensure continuity of internal controls regardless of any changes in the management or employee composition structure.
j) Focus on meeting all regulatory record keeping and reporting requirements while providing for timely updates that respond to changes in regulations.
k) Incorporate AML/CFT compliance into the job descriptions and performance evaluations of relevant personnel and provide for robust role based for those personnel to ensure sufficient expertise.
l) When applicable, Hardware Stores, may follow these general practices as part of their larger efforts to implement an RBA in their profession.
m) The type and extent of measures to be taken should be appropriate having regard to the risk of money laundering/ terrorism financing/ proliferation financing and the size of the business.
n) Hardware Stores' programmes against money laundering, terrorist financing and proliferation financing should be applicable to all branches and majority owned subsidiaries of the holding company.

5.3. The qualifications of the Compliance Officer shall:

a) be a fit and proper person.
b) Not have been convicted of a criminal offence in Eswatini.
c) Not have been convicted outside Eswatini of a criminal offence, which, if committed in Eswatini would have been a criminal offence.
d) Not be an un-rehabilitated insolvent.
e) Not be a subject of an investigation by a supervisory authority or an investigatory authority, and
f) Not have been a person holding a senior management position in a company which is disqualified from trading by a professional body or supervisory authority.

5.4. The Hardware Store's CRMP framework

a) The CRMP governance (s.5.4).
b) ML/TF/PF risks assessment and risk rating framework (s.2.5).
c) Customer due diligence controls (s3.8).
d) Targeted financial sanctions controls aimed at terrorist financing (s.6.2).
e) Targeted financial sanctions controls aimed at proliferation financing (s.6.3).
f) Politically Exposed person controls (s.4.3)
g) Account monitoring (s.8.4)
h) Reporting controls, (s.8.5) and
i) Record-keeping controls (s.7.5).

5.5. CRMP governance

Hardware Stores should document the CRMP governance controls in the CRMP document, which must indicate:

a) The roles, responsibilities, governance structures and oversight functions of the compliance officer, the compliance function, board of directors, senior management or other persons exercising the highest level of authority in relation to compliance with the MLFTP Act,2011, as amended and the Hardware Stores' CRMP.
b) Who the section 18 compliance officer is, and the level of competence and seniority that person holds. The Hardware Stores must be able to demonstrate that the section 18 compliance officer has sufficient competence and seniority.
c) Documented approval of the CRMP by board of directors, senior management or other persons exercising the highest level of authority.

d) The regular interval dates upon when the CRMP will be reviewed. The EFIU recommends that Hardware Store's review their CRMP annually or as and when the need arises, as the ML/TF/PF risks change continuously.

e) The process to implement the CRMP and its dissemination to employees. The Hardware Store's business could implement its CRMP through various controls which include, but are not limited to their policies, processes, systems, employees, and training.

f) The AML/CFT/PF training controls that apply within the Hardware Store's business.

g) The requirement to escalate AML/CFT/PF breaches in control measures to board of directors, senior management or other persons exercising the highest level of authority.

h) The remediation steps Hardware Stores must implement based upon the different AML/CFT/PF breaches.

5.6. Outsourcing and subcontracting arrangements

Where a hardware chooses to outsource or subcontract work to a third party it is still obliged to maintain appropriate risk management procedures to prevent ML/TF. This also requires the firm to consider whether the outsourcing or subcontracting increases the risk that it will be involved in, or used for, ML/TF, in which case appropriate controls to address that risk should be put in place.

a) Where a hardware contracts with a client, it remains responsible for ensuring that it undertakes CDD to the Act's standards, including maintaining the appropriate records even if execution of all or part of the client work is outsourced or sub-contracted out. Some aspects of CDD such as collecting documentary evidence can also be delegated to an outsourcer or sub-contractor, but the hardware remains responsible for compliance with Eswatini's legislation.

b) Regardless of any outsourcing or subcontracting arrangement, a company remains responsible for reporting any knowledge or suspicion of ML/TF that comes to it during its own business. However, a hardware is not responsible for reporting knowledge or suspicion that comes to the attention of the outsourcer or sub-contractor, where such knowledge or suspicion has not been passed on to the hardware. Although there is no legal obligation for an outsourcer or subcontractor to report knowledge or suspicion of ML/TF to the hardware, if such a suspicious activity report (SAR) is made, then the hardware should consider its own reporting obligations. When a sub-contractor is integrated into a company it may be appropriate for its relevant employees to be trained in the ML/TF procedures adopted by that company so that common standards can be observed.

6. Section 6: Targeted financial sanctions

6.1. Targeted financial sanctions Introduction.

Recommendation 6 requires each country to implement the targeted financial sanctions regimes to comply with the United Nations Security Council resolutions (UNSCRs or resolutions) relating to the prevention and suppression of terrorism and terrorism financing. FATF Recommendation 6 is intended to assist countries in implementing the targeted financial sanctions contained in the UNSCRs relating to the prevention and suppression of terrorism and terrorism financing:

a) UNSCR 1267(1999)
b) UNSCR 1373(2001); and
c) any future UNSCRs which impose targeted financial sanctions in the terrorist financing context.

These resolutions require countries to freeze, without delay, the funds, or other assets of, and to ensure that no funds or other assets are made available, directly, or indirectly, to or for the benefit of, any person or entity either.

d) designated by, or under the authority of, the United Nations Security Council (the Security Council) under Chapter VII of the Charter of the United Nations, or
e) designated by that country or by a supra-national jurisdiction pursuant to UNSCR 1373. Such measures may be either judicial or administrative in nature.

6.2. Targeted financial sanctions controls relating to terrorist financing.

a) Hardware Stores must detail the process to comply with the targeted financial sanctions regime aimed at terrorist financing in the CRMP document.

b) A targeted financial sanctions process must provide for:

i. The way the Hardware Stores will scrutinise client information to identify persons listed on a United Nations Security Council 1267 resolutions list, OFAC, EU

ii. The systems used and supporting processes for scrutinising client information.

iii. The freezing of accounts process that must be followed should a client or potential client be listed on a TF list.

iv. It is important to note that client information includes information regarding the client, prospective client, beneficial owner, person acting on behalf of the client and transaction/payment information.

6.3. Targeted financial sanctions controls relating to proliferation financing.

a) Hardware Store must document its process in place to comply with the targeted financial sanctions regime aimed at proliferation financing in the CRMP document.

b) A targeted financial sanctions process must provide for:

i. The way the Hardware Store's business will scrutinise client information to identify persons listed on a TF list as published in terms of UNSC Regulations.

ii. The systems used and supporting processes for scrutinising client information.

iii. The freezing process that must be followed should a client or potential client be listed on a sanction list.

iv. It is important to note that client information includes information regarding the client, prospective client, beneficial owner, person acting on behalf of the client and transaction/payment information.

6.4. Importance of an effective freezing regime

Effective freezing regimes are critical to combating the financing of terrorism and, as a preventive tool, accomplish much more than freezing terrorist-related funds or other assets present at any time. Effective freezing regimes also combat terrorism by:

a) Deterring non-designated persons or entities who might otherwise be willing to finance terrorist activity.
b) Exposing terrorist financing "money trails" that may generate leads to previously unknown terrorist cells and financiers.
c) Dismantling terrorist financing networks by encouraging designated persons or entities to disassociate themselves from terrorist activity and renounce their affiliation with terrorist groups.
d) Terminating terrorist cash flows by shutting down the pipelines used to move terrorist.
e) related funds or other assets.

6.5. Mechanism for implementation

Mechanisms for the implementation of the UNSC Resolutions include the circulation of the Designation or List by the United Nations Security Council Resolutions Implementation Committee to the EFIU, other supervisory authority, REP, UEDF, such other law enforcement agencies.

The EFIU or a supervisory body shall, upon receipt of the designations or sanctions list submitted to it under sub-regulation (4):

a) Circulate the designations or sanction list to reporting entities under its purview for their information and action,
b) Where necessary, provide guidance to reporting institutions holding funds or other assets of a designated person, in relation to their obligations under UNSC Regulations and
c) Ensure that the reporting institutions comply with the requirements of these UNSC Regulations

6.6. Authority to freeze

a) The Principal Secretary may either on his own motion or at the request of the Committee, make an order freezing the property or funds of a designated entity, whether held directly or indirectly by the entity or by a person acting on behalf of or at the direction of the designated entity, in accordance with the UNSC Regulations.
b) The freezing order shall include ongoing prohibition against the provision of funds or financial services to the designated entity against which the order is made.
c) A designation or sanctions list circulated by the Principal Secretary, or the Committee shall be deemed to authorise a reporting institution and any other institution which holds the property of a designated entity to freeze, until further notice.

6.7. Action to be taken on receipt of sanction lists:

A person to whom a designation or sanctions list is submitted, shall where applicable-

a) Take necessary steps to freeze the funds owned or controlled by the designated entity without delay and without notice to the entity,
b) Within twenty-four hours of detecting the funds and freezing the funds, file a suspicious transaction report with EFIU in such form as prescribed by the EFIU or in such form as may be prescribed by the committee.

A person who is required to act under the UNSC Regulations shall, without delay, inform the committee in writing, of the action taken.

6.8. Domestic list

The Committee shall compile a domestic list comprising of specified entities under section 28 of the Suppression of Terrorism Act.

The domestic list shall include the following information:

a) The name including any alias or title of the entity,
b) The place and date of birth, establishment, or incorporation,
c) The original or acquired nationality,
d) Passport number, identity card number or registration number,
e) Gender
f) Physical or postal address
g) Occupation,
h) Telephone number
i) Any other information which the committee consider relevant.

The Domestic list shall be circulated in the same manner as the sanction list.

The Committee shall review and where applicable, update the domestic list annually.

The Domestic list shall also be circulated to other states.

6.9. Publication of designations

a) The EFIU shall publish the domestic list on its website and make it available to the public an electronic version of the list.
b) The committee may adopt such measures or make such arrangement for the prompt publication and dissemination of the domestic list.

6.10. Third party publications

A designation or request for designation made by another country shall be transmitted through the foreign missions or the ministry of foreign affairs.

Upon receipt of request from other country for designation, the Mission or Ministry shall without delay submit request to the Principal Secretary for the consideration of the Principal Secretary who shall in turn transmit it to the Committee for a determination as to whether there are reasonable grounds to designate the entity in accordance with the Suppression of Terrorism Act, 2008

Where the Committee determines that there are reasonable grounds to designate that entity, the Principal Secretary shall without delay:

a) Make an order designating the entity,
b) Make an order freezing the assets of the entity; and

c) Circulate the order in accordance with UNSC Regulations

d) Proposal for designation to 1267/1989

The Committee shall also determine whether there are reasonable grounds to propose to the UNSCRs 1267/1989 Sanctions Committee a person or entity which-

e) Participate in the financing, planning, preparing, or perpetuating of acts or activities of terrorism.

The Committee shall determine whether there are reasonable grounds to propose and through the Chairperson, shall propose the name of the person or entity to the respective sanctions committee through the country's permanent mission to the UN.

6.11. Humanitarian exemption procedure for claiming:

A person whose assets have been frozen, such person or entity shall not withdraw any monies or deal with such property unless:

a) The property is necessary to cover the basic and necessary expenses or extraordinary expenses of the entity; and
b) The person or entity has applied for and obtained an authorisation from the Principal Secretary
c) The Principal Secretary shall approve the request where there are merits in the application.
d) The Principal Secretary shall prior to authorising withdrawal, notify the Sanctions Committee and request advise.
e) If after ten days of notification of the Sanctions Committee and in the absence of negative recommendations from the Sanctions Committee, the Principal Secretary shall authorise the withdrawal of such monies which may be reasonable to cover the basic and necessary expenses of the person or entity.

6.12. Application for de-listing

A designated entity may apply for de-listing by filing a petition with appropriate Sanctions Committee. Grounds for such application may be:

a) Mistaken identity
b) Relevant and significant change of facts or circumstances including the inclusion of the Applicant in a witness protection program.
c) The death, dissolution, or liquidation of designated entity or,
d) Any other circumstances which would show that the basis of the designation no longer exists.

If the Sanction Committee removes the name of the entity from the sanction list, the Principal Secretary shall notify the Accountable Institutions within 24 hrs of the removal and direct Accountable Institution to remove the name from the list circulated.

6.13. Screening

a) Hardware Stores must be able to determine whether they have a sanctioned person or entity as a client or whether a prospective client is a sanctioned person or entity to determine their exposure to TFS-related obligations. This implies that accountable institutions which are likely to encounter sanctioned persons or entities can screen clients and prospective clients against the relevant sanctions lists. This should be done during the client-take-on process as well as subsequently as and when the UNSC adopts new TFS measures or expand existing ones.

b) Hardware Stores must therefore determine the likelihood that their client base and intended target market may include sanctioned persons or entities. This should assist the Hardware Stores in determining the amount of effort and resources it requires to determine whether they have sanctioned persons or entities as a client or whether prospective clients are sanctioned persons or entities. Hardware Stores that have business relationships with foreign persons and entities are more vulnerable to dealing with sanctioned persons and entities.

c) Hardware Stores should be mindful of the fact that failure to comply with TFS obligations is a criminal offence under section 89 of the MLFTP Act.

6.14. Obligations to report.

a) Adherence to the Targeted Financial Sanctions (TFS) obligations, are imposed on all Hardware Stores undertaking the activities under recommendation 22 and failure to comply constitutes an offence in in terms of Reg.27 of the Anti-Money Laundering (UNSCR) Regulations of 2016.
b) In terms of the TFS obligations, no person may directly or indirectly, in whole or in part, and by any means or method enter any transaction, facilitate a transaction, or assist in a transaction with an entity identified on a specified resolution, as determined by the Security Council of the United Nations.
c) Hardware Stores must report to the EFIU, the property in the Hardware Store's control which is owned or controlled by or on behalf of a person or an entity identified in the sanctions list.
d) The Suppression of Terrorism Act requires Hardware Stores, to file a report with the EFIU if the Hardware Stores or anyone it employs of the Hardware Store's business knows that it possesses, or controls property linked to terrorism or to entities that are sanctioned.

e) The knowledge about the origin and ownership of the property in question is based on fact and should be acquired with reference to an objective set of circumstances or facts (as opposed to a suspicion that is formed subjectively).

f) These UNSC Resolutions are the only sanctions lists related to terrorist activities which are legally recognised within the country and can be accessed on the United Nations website.

g) In terms of regulations 12(1)(b), a report must be sent to the EFIU as soon as possible but no later than 24 hrs after it has been established that the Hardware Store's business has property associated with terrorist and related activities in its possession or under its control.

h) Hardware Stores must note that this reporting period is effective from the time the institution becoming aware of such report, and it may not add additional time frames for its internal sanction/watch list screening tools and processes, internal transactional monitoring alert system processes, and/or internal investigation and review processes to the prescribed reporting period.

6.15. Identifying information

a) For the effective implementation of an asset freeze, robust identifying information is essential. At the extreme end of the scale, poor quality identifiers are an obstacle to the enforcement of an asset freeze. Single name identifiers represent problems for enforcement.

b) Best efforts should therefore be made to ensure as much identifying information as possible is provided upon designation, and that such information be updated as more identifying data become available.

7. Section 7: Record Keeping

7.1. Record keeping Introduction.

Hardware Dealers are to adopt appropriate record keeping guidelines in accordance with the FATF Recommendations and the Money Laundering and Financing of Terrorism (Prevention) Act, 2011. The nature and size of the business will determine the type of documents to be kept, and the method that will be used. The system used to retain the documents should be eligible enough to allow the company to be able to reconstruct records in the event a supervisory authority requests the Hardware Store's business to do so. And the customer records to be kept should be relevant to the customer's profile. The FATF recommendation outlines the period that documents need to

be kept and the way the documents shall be kept, as well as the MLFT(P) Act that prescribes how the documents are to be kept and penalises non – compliance with the Act itself.

7.2. Record keeping international standards.

a) According to FATF R.11, Hardware Stores should be required to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) to provide, if necessary, evidence for prosecution of criminal activity.

b) Hardware Stores are required to keep all records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licences or similar documents), account files and business correspondence, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions), for at least five years after the business relationship is ended, or after the date of the occasional transaction.

c) Hardware Stores are required by law to maintain records on transactions and information obtained through the CDD measures. The CDD information and the transaction records should be available to domestic competent authorities upon appropriate authority.

7.3. Hardware Dealers record keeping requirements.

a) Hardware Stores should establish and maintain records of:
    i. the identity of a person obtained in accordance with section 6 of the MLTFP Act,
    ii. All transactions carried out by it and correspondence relating to the transactions as is necessary to enable the transaction to be readily reconstructed at any time by the EFIU or competent authority and shall contain particulars as the Minister may by regulation prescribe.
    iii. All reports made to the EFIU under section 12; and,
    iv. Enquiries relating to money laundering and financing of terrorism made to it by the EFIU.

b) The records mentioned in subsection (1) shall be kept for a minimum period of five years from the date:
    i. the evidence of the identity of a person was obtained,
    ii. of any transaction or correspondence, and
    iii. the account is closed or business relationship ceases, whichever is the later.

c) The records established and maintained for purposes of subsection (1) shall be –

i. sufficient to enable the transaction to be readily reconstructed at any time by the SFIU or competent authority to provide, if necessary, evidence for prosecutions of any offence; and,

ii. maintained in a manner and form that will enable the accountable institution to comply immediately with requests for information from the law enforcement or EFIU.

d) Where any record is required to be kept under this Act, a copy of it, with the appropriate back – up and recovery procedures, shall be kept in a manner as the Minister may by Regulation prescribe.

e) The records maintained under subsection (1) shall be made available upon request to the EFIU, or a competent authority for purposes of ensuring compliance with this Act and for purposes of an investigation or prosecution of an offence.

7.4. Failure to maintain records.

Hardware Stores that fail to perform the below commits and offense:

a) Keep record of information in terms of Section 8(1),

b) Keep such records in accordance with Section 8(2, or

c) Comply with the provisions of Section 8(3).

7.5. Record keeping controls.

Hardware Stores must document their record-keeping process. It is the EFIU's view that this process should clearly indicate records access and confidentiality controls. This process could include:

a) What records must be kept,

b) In what format will these records be kept (e.g., hard copies or electronic records)

c) The period for which records must be kept,

d) If the records are kept by a third party, details thereof as prescribed in terms of Money Laundering and Terrorist Financing Act.

8. Section 8: Suspicious transactions reporting

8.1. STR introduction

Hardware Stores must have a policy that will establish procedures for statutory obligations on suspicious activity reporting to the EFIU. These procedures should also reflect the principle of confidentiality, ensure that investigation is conducted swiftly and that reports contain relevant information and are produced and submitted in a timely manner. The Compliance Officer must

ensure prompt disclosures where funds or other property that is suspected to be the proceeds of crime remain in an account.

8.2. Identification, investigation, and reporting of suspicious transactions.

a) The process for identifying, investigating, and reporting suspicious transactions to the EFIU should be clearly specified in the accountable institution's policies and procedures and communicated to all personnel through regular training. These policies and procedures must contain a clear description for employees of their obligations and instructions for the analysis, investigation, and reporting of such activity within the institution as well as guidance on how to complete such reports.

b) Where Hardware Stores suspect, or has reasonable grounds to suspect, that funds are the proceeds of crime or are related to terrorist financing, it shall report its suspicions not later than 2 working days to the EFIU. Hardware Stores should have the ability to flag unusual movement of funds or transactions for further analysis.

c) Further, Hardware Stores should have appropriate case management systems so that such funds or transactions are scrutinised in a timely manner to whether the funds or transaction are suspicious. In addition to reporting the suspicious activity Hardware Stores must ensure that appropriate action is taken to adequately mitigate the risk of the institution being used for criminal activities. This may include reviewing the risk classification of the customer or account or of the entire relationship itself.

8.3. Terrorist property reporting (TPR)

As discussed above, the UNSCR (2016) provides for the reporting and freezing without delay any suspicions relating to funds or assets linked to terrorist financing.

a) Hardware Stores must be able to identify and enforce provisions of the UNSCR which require to freeze without delay any assets or funds suspected to be linked to institutions or persons that have been classified as designated entities or individuals in terms of the relevant Eswatini legislations before establishing a business relationship or carrying out an occasional transaction with new customers, Hardware Store's must screen customers against lists of known or suspected terrorists issued by competent national and international authorities. Likewise, ongoing monitoring should verify that existing customers are not entered into these same lists.

b) Hardware Stores must have policies that detail out the process and procedures under TPR and employees should be trained accordingly.

8.4. Accounts monitoring

Hardware Stores' businesses must include processes to monitor client transactional activity in the CRMP document, which indicates:

a) The manual or automated processes must put in place for account monitoring in terms of the Act, to determine whether the transaction is consistent with the client's business and risk profile.

b) The process must put in place for examining complex and unusually large transactions and unusual patterns of transactions which have no apparent business or lawful purpose, as well as the process to keep written findings of the business' decisions in this regard.

8.5. Reporting controls

Hardware Stores must document reporting process in the CRMP document which sets out:

a) The end-to-end internal process for identifying possible reportable transactions, analyse and report transactions to the EFIU, in terms of sections 12, section 12bis. and Suppression of Terrorism Act of 2008, where applicable. This would include who must submit the report, and the periods within which the reports must be submitted to the EFIU or law enforcement.

b) The process in place to keep written findings of the Hardware Store's decisions to report or not.

c) A clear instruction on tipping off and the non-disclosure of STRs reports to other persons.

8.6. Cash threshold reporting.

The EFIU has issued a guidance to accountable institutions on this obligation and reference must be made to it. This guideline is found in the EFIU website.

END

9. Annexure1: ML Red Flags

ML Red Flags

These are not exhaustive:

a) Client wants to remain anonymous,

b) The client refuses to identify a source for funds or provides information that is false, misleading, or substantially incorrect,

c) Client makes large cash deposits their accounts/ card,

d) Client makes large cash payments for hardware material,

e) Customer makes cash deposit or purchase then request refunds from hardware account or card through a bank transfer or other electronic funds transfer methods.

f) Customer negotiates a purchase for market value or above asking price, but records a lower value on documents, paying the difference “under the table”.

g) Customer frequently deposits funds into an account/ card of a nominee such as an associate or a relative (other than a spouse).

h) Customer’s documentation to ascertain identification, support income or verify employment or financial statement is provided by an intermediary who has no apparent reason to be involved, or not provided at all.

i) Customer seems unconcerned with terms of credit or costs associated with completion of a transaction, and Customer frequently uses trust accounts for transactions where it may not make business sense to do so.

j) Client approaches different staff to conduct transactions.

k) Client exhibits nervous behavior or has a defensive stance to questioning.

l) Client makes inquiries/statements indicating a desire to avoid reporting or tries to persuade the reporting entity not to file/maintain required reports.

m) The transactional activity is inconsistent with the client’s apparent financial standing, their usual pattern of activities or occupational information.