VIRTUAL CLC
Career Ready Academy
virtualclc.co.za

Financial Intelligence Centre Act as Amended 2022

6 CPD Hours

All Classes of Business

Author: Anna Bouhail

Copyright: Compliance and Learning Center (Pty) Ltd

Date: January 2024

Copyright Protection Notice

© 2023, Compliance and Learning Center (Pty) Ltd. All rights reserved.

No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law.

For permission requests, write to the publisher, at ceo@virtualclc.co.za

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

Table of Contents

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

Lesson 1 The Money Laundering Landscape

1.1 Introduction

The realm of financial transactions is vast and complex, serving as both a catalyst for global economic growth and, unfortunately, a conduit for illicit activities. At the heart of this paradox lies the issue of money laundering, a sophisticated crime that poses significant challenges to the integrity of financial systems worldwide.

This lesson introduces the intricate landscape of money laundering, exploring its mechanisms, the legal frameworks established to combat it, and the pivotal role that financial institutions and regulatory bodies play in detecting and preventing these unlawful activities. By delving into the origins, methods, and impacts of money laundering, we aim to provide a comprehensive understanding of the threats it presents and the collective efforts required to safeguard the financial sector from its detrimental effects.

1.2 Glossary

This glossary provides definitions and explanations for key terms related to Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT), along with associated regulatory, financial, and professional entities and concepts, serving as a foundational resource for understanding the complex landscape of financial regulation and compliance.

- **AML/CFT:** Anti-Money Laundering/Counter-Terrorist Financing. A set of procedures, laws, and regulations designed to prevent criminals from disguising illegally obtained funds as legitimate income.
- **CASP:** Crypto Asset Service Provider. Entities that provide services related to digital currencies, such as exchanges, wallet services, and financial transfers.
- **CIBA:** Chartered Institute for Business Accountants. The professional body formerly known as the Southern African Institute for Business Accountants.
- **FATF:** Financial Action Task Force. An intergovernmental organization founded to develop policies to combat money laundering and terrorist financing.
- **FIC:** Financial Intelligence Centre. The national agency responsible for the collection, analysis, and dissemination of financial intelligence to combat money laundering and terrorist financing.
- **IFAC:** International Federation of Accountants. The global organization for the accountancy profession, dedicated to serving the public interest by strengthening the profession and contributing to the development of strong international economies.
- **IRBA:** Independent Regulatory Board for Auditors. The regulatory body overseeing the auditing profession in a specific jurisdiction, ensuring compliance with standards and ethical practices.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

- **MER:** Mutual Evaluation Report. A detailed assessment report that evaluates a country's compliance with the FATF recommendations on anti-money laundering and counter-terrorist financing measures.
- **NPO:** Nonprofit Organisation. An organization dedicated to furthering a particular social cause or advocating for a shared point of view, not operating for the profit or gain of its members.
- **POCDATARA:** Protection of Constitutional Democracy Against Terrorism and Related Activities Amendment Act, 23 of 2022. Legislation aimed at updating and strengthening laws against terrorism and related activities within a constitutional framework.
- **PCC:** Public Compliance Communications. Communications issued by regulatory bodies to provide guidance and information on compliance-related matters to the public and regulated entities.
- **SAIBA:** Southern African Institute for Business Accountants. The original name of the Chartered Institute for Business Accountants, a professional body for accountants.
- **TCSP:** Trust and Company Service Providers. Entities that provide administrative services to trusts and companies, including acting as agents in forming legal entities, serving as, or arranging for another person to serve as, a director or secretary of a company.
- **VDR:** Voluntary Disclosure Report. A report through which individuals or entities voluntarily disclose information to regulatory authorities, often related to financial misstatements or tax evasion, in exchange for certain legal protections or concessions.

1.3 What Money Laundering Is

Following our enthusiastic leap into the world of financial intelligence, let's pause for a moment to unravel the concept of money laundering—a term that's often thrown around but not always fully understood. At its core, money laundering is the devious art of making ill-gotten gains appear legal and legitimate. Imagine a villain in a thriller movie, trying to disguise their loot from a heist as earnings from a legitimate business. That's money laundering in action.

Crooks misuse the commercial system with alarming creativity. For instance, they might use a legitimate-looking business, like a car wash or a restaurant, to blend their dirty money with the day's genuine earnings. On paper, it looks like the business is booming, but in reality, it's just a façade to clean their criminal proceeds. Another clear example is the use of shell companies—entities that exist only on paper, with no real business operations. These shell companies can hold accounts, own property, and conduct transactions, all while the true owners remain hidden behind layers of secrecy. Through these and other methods, money launderers exploit the commercial system to give their illicit funds a veneer of respectability, making it a challenge for authorities to trace and tackle.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

This misuse not only undermines the integrity of financial systems but also fuels further criminal activities by allowing bad actors to enjoy their proceeds without repercussion. Understanding these mechanisms is crucial for anyone looking to combat financial crime effectively. Through this course, we'll delve deeper into these examples and more, equipping you with the knowledge to identify and prevent such abuses in the commercial system.

1.3.1 Impact of Money Laundering on Economies and Societies

Money laundering does not just complicate the lives of financial crime investigators; it strikes at the very heart of our economies and societies. The ramifications of these illicit activities are vast and multifaceted, affecting everything from global economic stability to the well-being of individual communities.

Firstly, money laundering can distort economic data, leading to misguided policy decisions. When illicit funds flood into legitimate markets, they can inflate asset prices, such as real estate, creating bubbles that risk devastating crashes. For example, in some cities, laundered money poured into property markets has driven up home prices beyond the reach of average families, contributing to housing crises.

Moreover, money laundering facilitates corruption and organized crime, eroding the rule of law and public trust in institutions. This erosion can deter foreign investment, as investors become wary of entering markets seen as corrupt or unstable. The economic consequences are dire: reduced investment means slower growth, fewer jobs, and diminished prosperity.

On a societal level, the impact is equally grievous. By enabling criminal enterprises to profit from their activities, money laundering indirectly supports drug trafficking, human trafficking, terrorism, and other crimes that prey on communities and vulnerable populations. The profits from these activities can then be used to expand criminal operations, creating a vicious cycle of crime and laundering.

Understanding these impacts is crucial for appreciating the significance of the battle against money laundering. It's not just about tracking down illicit funds; it's about protecting the very fabric of our societies and ensuring a fair and just economic system for all. Through this course, we aim to arm you with the knowledge and skills to contribute meaningly to this fight, safeguarding our future from the corrupting influence of laundered money.

1.4 Terrorism Activities and misuse of the Financial System

Terrorism activities encompass a broad range of acts intended to instill fear, cause harm, and disrupt societies for political, religious, or ideological objectives. These can range from bombings, shootings, and kidnappings to cyber-attacks and other forms of violence aimed at civilians, infrastructure, or governments. The financial underpinnings of these activities are crucial yet often overlooked. Without funding, the operational capacity of terrorist groups to plan, execute, and sustain their campaigns would be significantly diminished.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

Criminals and terrorist organizations ingeniously exploit the financial system to support their activities. They rely on a mixture of legal and illicit funding streams, including state sponsorship, donations from sympathizers, extortion, smuggling, drug trafficking, and other forms of organized crime. However, simply acquiring funds is only part of their challenge; they must also move and use these funds without detection. This is where the misuse of the financial system becomes evident.

One common method is the use of informal value transfer systems, such as the hawala system, which operates on trust and does not leave a paper trail like conventional banking transactions. Terrorists also use front companies, charities, or legitimate businesses to disguise the flow of funds, blending them with legitimate financial activities to avoid arousing suspicion. Additionally, cryptocurrencies and other digital currencies offer anonymity and can be used to transfer funds across borders quickly and without the oversight typically associated with traditional banking systems.

For example, a terrorist group might establish a charity that appears to support a noble cause, soliciting donations from unsuspecting individuals and organizations worldwide. These funds, however, are then diverted to finance terrorist operations. Similarly, purchasing small amounts of prepaid cards or mobile credits can be a way to transfer value without attracting attention, demonstrating the diverse and innovative methods terrorists use to finance their activities.

Understanding these tactics is vital for financial institutions, law enforcement, and individuals involved in combating terrorism financing. It highlights the importance of vigilance, robust financial intelligence, and international cooperation in identifying and disrupting the financial networks that underpin terrorist operations. Through this course, we'll explore these concepts further, providing you with the tools and knowledge to recognize and counteract the financial strategies employed by terrorists.

1.5 Proliferation Financing

Proliferation financing involves providing funds or financial services that contribute to the development, acquisition, or transfer of weapons of mass destruction (WMDs), as identified by relevant United Nations Security Council Resolutions. The Financial Action Task Force (FATF) emphasizes the need for countries and private sector entities to identify, assess, and mitigate risks associated with proliferation financing, ensuring that financial systems do not inadvertently support WMD proliferation networks.

1.6 Definitions

Here are definitions as per the Financial Intelligence Centre Act (FICA) essential for understanding the regulatory framework and obligations within the financial sector:

- **Money laundering:** Money laundering is the process that criminals use to launder their funds so that the proceeds they have acquired from illicit (illegal) activities appear to be legitimate.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

- **Terrorist financing:** Terrorist financing is the process of funding terrorists, terrorist acts or terrorist organisations.
- **Proliferation financing:** Proliferation financing is where individuals, entities, countries or governments raise funds in order to assist with their purchasing of weapons of mass destruction.
- **Client:** A client may be regarded as anyone who uses the services of an accountable institution. Client categories include natural persons, companies, close corporations, trusts and partnerships.
- **Business Relationship:** A business relationship is an arrangement between a client and an accountable institution for concluding either a single transaction or transactions on a regular basis. Accountable institutions are listed in the Table following.

1.7 South African Money Laundering Laws

In a globalized economy, financial systems and markets are intricately interconnected. Money can move across borders with ease, and while this facilitates legitimate business and investment, it also opens the door to money laundering on a scale previously unimaginable. Strong safeguards are not just a national requirement but a global necessity. Without them, money launderers can exploit the gaps and discrepancies between different countries' regulatory systems, moving illicit funds through jurisdictions with weaker laws to clean their money.

This exploitation undermines economic stability, as laundered money can distort asset prices, fuel corruption, and finance crime and terrorism. It erodes public trust in financial institutions and can attract sanctions and other punitive measures from international bodies, harming a country's reputation and its ability to participate in the global financial system. For these reasons, countries like South Africa have implemented robust legal frameworks to combat money laundering, ensuring they are not seen as weak links in the global fight against financial crime.

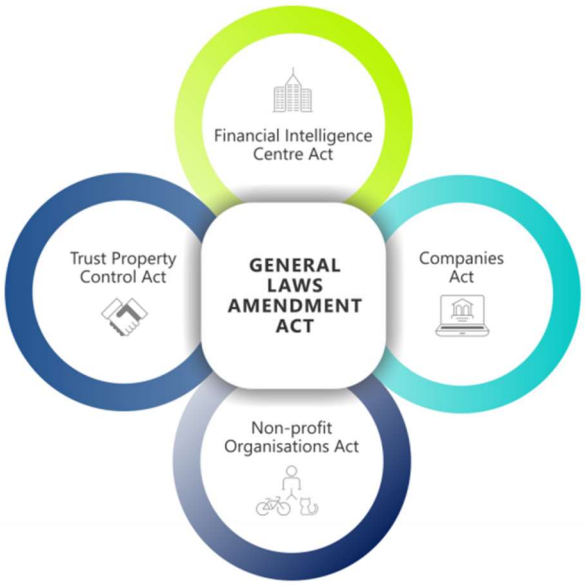
South Africa has several key pieces of legislation designed to combat money laundering and associated financial crimes:

- **Prevention of Organised Crime Act (POCA):** POCA provides for the prevention of organized crime, the introduction of measures to combat organized crime, the prohibition of certain activities associated with organized crime, and the forfeiture of property derived from organized crime. It includes provisions for dealing with the proceeds of crime and aims to prevent money laundering by making it an offense to possess or transfer property known to be derived from criminal activities.
- **Financial Intelligence Centre Act (FICA):** FICA establishes the Financial Intelligence Centre and imposes certain duties on institutions and other persons who might be dealing with money laundering. Its main aim is to identify the proceeds of unlawful activities and combat money laundering activities. FICA requires institutions to implement various measures such as client identification and verification, record-keeping, reporting of suspicious and unusual transactions, and compliance with FICA regulations.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

- **Protection of Constitutional Democracy Against Terrorist and Related Activities Act (POCDATARA):** This act specifically targets terrorism financing but is also relevant to money laundering, as it criminalizes the provision and collection of funds for terrorist activities. It outlines measures for preventing the use of the South African financial system for such purposes, including asset freezing and other financial sanctions against individuals and entities involved in terrorism.
- **General Laws Amendment Act (Anti-Money Laundering and Counter-Terrorism Financing):** While not a standalone act, this refers to amendments made to existing laws, including FICA, aimed at strengthening South Africa's anti-money laundering (AML) and counter-terrorism financing (CTF) measures. These amendments are designed to address new and emerging threats and to ensure compliance with international standards set by bodies such as the Financial Action Task Force (FATF).

1.8 The General Laws Amendments Act



In a significant stride toward fortifying its Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) framework, South Africa enacted the General Laws Amendment Act on 6 January 2023. This legislative action was catalyzed by the Mutual Evaluation Report issued by the Financial Action Task Force (FATF) in October 2021, which highlighted crucial areas needing enhancement within the country's AML/CFT measures. The Amendment Act, demonstrating South Africa's commitment to international compliance, brought forth substantial changes across several laws, including the Financial Intelligence Centre Act (FICA), Trust Property Control Act, Companies Act, and Nonprofit Organisations Act.

1.8.1 Key Amendments and Their Implications

Broadening the Scope of Beneficial Ownership: The amendments introduced by the General Laws Amendment Act aim to establish a more transparent and accountable system for identifying and reporting beneficial ownership within corporate entities such as trusts and companies. These changes are pivotal in closing the gaps that previously allowed for the concealment of illicit funds and the evasion of financial scrutiny.

1.8.2 Amendments to the Financial Intelligence Centre Act (FICA)

The FICA amendments are integral to the enhanced AML/CFT regulatory framework, focusing on:

- Refinement of Key Definitions: The act refined definitions related to beneficial ownership and introduced the concept of "prominent influential persons," broadening the scope for due diligence.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

- Expansion of the Financial Intelligence Centre's Objectives and Functions: These amendments have enabled the Centre to access a wider range of information, including forensic data, thereby strengthening its investigative capabilities.
- Strengthening Due Diligence and Information Disclosure: Enhanced due diligence measures and the clarification of procedures for verifying the authenticity of provided information have been emphasized.
- Enforcement and Compliance Measures: The act has introduced provisions for more robust enforcement mechanisms, including administrative sanctions for non-compliance.

1.8.3 Amendments to the Trust Property Control Act

This act has undergone substantial revisions to ensure trustees are held to stricter standards, including:

- Enhanced Definitions and Requirements for Trustees: New definitions and obligations for trustees aim to prevent misuse of trusts for illicit purposes.
- Maintenance of Beneficial Ownership Registers: Trustees are now required to maintain detailed records of beneficial ownership, improving transparency and accountability in trust administration.
- Regulatory Oversight and Compliance: The amendments provide clear guidelines for the removal of trustees who fail to meet the stipulated requirements, enhancing the integrity of trust management.

1.8.4 Overview of Amendments to the Companies Act

As part of South Africa's comprehensive approach to bolster its Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) framework, significant amendments were made to the Companies Act. These amendments, enacted via the General Laws Amendment Act, signify a pivotal advancement in corporate regulation, particularly in the arena of beneficial ownership transparency. The key modifications introduced are designed to ensure that the Companies and Intellectual Property Commission (CIPC) maintains accurate and up-to-date records of beneficial ownership, thereby aligning South Africa with global standards set forth by the Financial Action Task Force (FATF).

<u>Key Amendments to the Companies Act</u>

Definition of "Beneficial Owner": A clear definition has been inserted to identify individuals who, directly or indirectly, ultimately own or exercise control over a company. This encompasses those holding significant interests or rights within the company, including voting rights or the ability to appoint or remove board members.

- **Record-Keeping and Reporting Requirements:** Companies are now obligated to maintain a record of their beneficial owners and report any changes within specified timelines. This record must be filed with the CIPC, ensuring a transparent trail of ownership and control.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

- **Prohibition of Certain Individuals:** The amendments explicitly prohibit individuals convicted of money laundering, terrorist financing, or proliferation financing activities from serving as company directors, reinforcing the integrity of corporate governance.

Beneficial Ownership Reporting

From 1 April 2023, companies are required to report beneficial ownership information to the CIPC. This initiative is set to be supported by new regulations detailing the processes and formats for such reporting, ensuring standardization and ease of compliance.

Classification of Companies

The amendments distinguish between 'affected companies' and 'companies which are not affected':

- **Affected Companies:** These include regulated companies as defined in section 117(1)(i) and private companies under the control or subsidiary of a regulated company due to specific circumstances. Affected companies must maintain a register of their beneficial owners.
- **Companies Not Affected:** While not required to maintain a register, these companies must still provide beneficial ownership information to the Commissioner in a specified format.

Understanding Beneficial Ownership

The concept of beneficial ownership is crucial for identifying the natural persons who ultimately own or control a company. This extends beyond direct ownership to include control exercised through various means, such as through a chain of ownership or control over company decisions. The definition is broad, encompassing individuals who influence the company through significant shareholdings, voting rights, or board appointments. This nuanced understanding of beneficial ownership aims to peel back the layers of corporate structures to reveal the actual individuals exerting control, crucial for tackling financial crimes effectively.

1.8.5 Overview of Amendments to POCDATARA

The POCDATARA Amendment Act, 23 of 2022, signifies a critical advancement in South Africa's legislative framework for combating terrorism and its financing. This Act amends the Protection of Constitutional Democracy Against Terrorism and Related Activities Act of 2004, aiming to address the evolving nature of terrorist threats, including the rise of cyberterrorism. These amendments are designed to tighten the existing legal provisions and introduce more robust mechanisms for the enforcement of financial sanctions against entities supporting terrorist activities.

Expansion to Include Cyberterrorism

One of the significant expansions brought about by the POCDATARA Amendment Act is the inclusion of cyberterrorism within its scope. This reflects a recognition of the modern terrorist landscape, where digital platforms can be exploited to carry out or support terrorist acts. By encompassing cyberterrorism, the Act ensures that the legal framework remains relevant and capable of addressing threats in the digital age.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

Refinement of the Offense of Terrorist Financing

The amendments provide a more detailed definition of terrorist financing, clarifying the scope of what constitutes financial support to terrorist activities. This refinement aims to close loopholes that could be exploited to funnel funds to terrorist organizations under the guise of legitimate transactions. By clearly delineating the boundaries of terrorist financing, the Act enhances the ability of law enforcement and financial institutions to identify and intercept such funds.

Improved Processes for Implementing Financial Sanctions

A crucial aspect of the POCDATARA Amendment Act is the introduction of improved processes for the implementation of financial sanctions against individuals or entities supporting terrorist organizations. These processes are designed to ensure swift and effective action to freeze assets and block financial transactions linked to terrorism. The enhanced framework facilitates better coordination among financial institutions, regulatory bodies, and law enforcement agencies, ensuring a united front against the financing of terrorism.

1.9 Understanding the Financial Intelligence Centre (FIC) Framework

The Financial Intelligence Centre (FIC) plays a pivotal role in South Africa's fight against money laundering, terrorist financing, and other financial crimes. As the central nucleus of the country's anti-money laundering (AML) and counter-terrorist financing (CFT) efforts, the FIC operates within a complex ecosystem involving various stakeholders and regulatory bodies. This section outlines the key role players within the FIC framework and examines the contributions of other regulators and institutions in policing and administering this framework.

1.9.1 Key Role Players within the FIC Framework

1. Financial Intelligence Centre (FIC)

At the heart of the AML/CFT framework, the FIC is responsible for collecting, analyzing, and distributing financial intelligence to combat money laundering, terrorist financing, and other threats to the financial system. The FIC acts as a conduit between financial institutions and law enforcement, ensuring that valuable financial data is appropriately leveraged to detect and disrupt illicit financial flows.

2. Accountable Institutions

Accountable institutions include banks, financial services providers, estate agents, and attorneys, among others, which are obligated under the FIC Act to implement stringent AML/CFT measures. These measures include customer due diligence, record-keeping, and the reporting of suspicious and unusual transactions directly to the FIC.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

1.9.2 Supporting Regulators and Institutions

Financial Action Task Force

The Financial Action Task Force (FATF) is a crucial international body established to combat money laundering, terrorist financing, and the proliferation of weapons of mass destruction through the promotion of global policy and standard-setting measures. South Africa, a member since June 2003, has actively engaged in FATF's mutual evaluations to assess its compliance with anti-money laundering (AML) standards, leading to actionable recommendations to improve its financial system's integrity.

The most recent evaluation (April 2019 to June 2021) culminated in the Mutual Evaluations Report (MER) published in October 2021, acknowledging South Africa's robust legal framework against financial crimes but also highlighting areas needing significant enhancement. Following these recommendations is vital for South Africa to maintain its international financial reputation and mitigate potential negative impacts on economic and transactional relationships. In pursuit of these objectives, South Africa has initiated legislative amendments and measures to address deficiencies and fortify its financial system against corruption, fraud, and terrorism.

South African Reserve Bank (SARB)

The SARB oversees banks and certain financial institutions, ensuring they comply with AML/CFT regulations. It plays a crucial role in maintaining the integrity and stability of the financial system and works closely with the FIC to enforce compliance among regulated entities.

Financial Sector Conduct Authority (FSCA)

The FSCA is tasked with regulating market conduct and ensuring fair treatment of consumers within the financial services sector. It also enforces AML/CFT compliance among non-banking financial institutions and works in tandem with the FIC to uphold high standards of financial integrity.

National Treasury

As the executive authority responsible for economic policy, the National Treasury plays a strategic role in the formulation of AML/CFT laws and regulations. It ensures that the country's financial regulatory framework aligns with international standards and best practices.

South African Revenue Service (SARS)

SARS is instrumental in identifying tax evasion schemes that may signal money laundering activities. It shares relevant financial intelligence with the FIC, aiding in the broader effort to detect and prevent financial crimes.

Directorate for Priority Crime Investigation (Hawks)

The Hawks handle the investigation of organized crime, economic crimes, and corruption. As a key law enforcement partner, they utilize financial intelligence provided by the FIC to pursue investigations into money laundering and terrorist financing.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

Independent Regulatory Boards

Various independent regulatory boards, specific to professions such as legal and accounting, ensure their members adhere to AML/CFT obligations. These boards collaborate with the FIC to promote compliance within their respective sectors.

1.10 Accountable Institutions

The FIC Act introduces a regulatory framework of measures requiring certain categories of business to fulfil compliance obligations. These compliance obligations are critical to assisting in identifying and disrupting money laundering, terrorist and proliferation financing. The FIC Act deems these categories of business, called accountable institutions, as being vulnerable to being abused by criminals for money laundering and terrorist financing purposes.

All FIC Act compliance obligations are premised on institutions implementing a risk-based approach to combating money laundering and terrorist financing.

- **Legal Practitioners:** This includes attorneys (including conveyancers and notaries) practicing for their own account, advocates, and commercial juristic entities as defined by the Legal Practice Act 2014.
- **Business and Trust Service Providers:** Individuals or entities involved in preparing or carrying out transactions for a client related to the organization, operation, or management of companies, external companies, foreign companies, close corporations, trusts, acting as a nominee, or creating trust arrangements.
- **Estate Agents:** As defined in the Estate Agency Affairs Act 1976.
- **Authorised Users of an Exchange:** Defined in the Financial Markets Act 2012.
- **Collective Investment Scheme Managers:** Registered in terms of the Collective Investment Schemes Control Act 2002, excluding those only conducting business in Part VI of that Act.
- **Banks and Financial Institutions:** This includes entities carrying on the business of a bank as defined in the Banks Act 1990, mutual banks, and cooperative banks.
- **Life Insurance Businesses**: As defined in the Insurance Act 2017, excluding reinsurance business.
- **Gambling Service Providers:** Those making available a gambling activity requiring a license issued by the National Gambling Board or a provincial licensing authority.
- **Foreign Exchange Dealers:** Entities dealing in foreign exchange.
- **Credit Providers:** Including those defined in the National Credit Act 2005, and those providing credit excluded from the application of this Act.
- **Financial Services Providers:** Those requiring authorisation to provide advice or intermediary services related to the investment of any financial product, excluding certain insurance and medical scheme activities.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

- **Issuers of Travelers Cheques and Similar Instruments**: Entities involved in issuing, selling, or redeeming travelers' cheques, money orders, or similar instruments.
- **The South African Postbank Limited**: Specifically referred to in the South African Postbank Act 2010.
- **Money or Value Transfer Providers**: Entities involved in the business of transferring money or value.
- **Dealers in High-Value Goods:** Those dealing in goods where transactions involve payments of R100,000 or more.
- **The South African Mint Company:** Limited to its distribution of non-circulation coins in retail trade for transactions involving payments of R100,000 or more.
- **Crypto Asset Service Providers:** Those involved in activities such as exchanging crypto assets for fiat currency or vice versa, exchanging one form of crypto asset for another, transactions transferring crypto assets, safekeeping or administration of crypto assets, and provision of financial services related to an issuer's offer or sale of a crypto asset.
- **Clearning System Participants:** Defined in the National Payment System Act 1998, facilitating or enabling the origination, receipt, or intermediary services in receiving or transmitting electronic funds transfer.

1.10.1 Complex Money Laundering Scheme Involving Multiple Institutions

Stage 1: Placement through Banks and Foreign Exchange Dealers

- Initial Deposit: The launderer starts by depositing illicit cash into a bank (Institution 6) in small amounts to avoid triggering mandatory reporting requirements. This is often done through multiple accounts under false identities.
- Currency Exchange: The launderer uses a foreign exchange dealer (Institution 10) to convert the money into a less suspicious form, such as foreign currency or digital assets, further complicating the trail.

Stage 2: Layering through Investment Schemes and Insurance Companies

- Investment in Mutual Funds: The launderer approaches a collective investment scheme manager (Institution 5) to invest the now-disguised funds into mutual funds or other collective investments, blending the illicit funds with legitimate capital.
- Insurance Policies: Part of the funds is used to purchase long-term insurance policies (Institution 8), with the launderer often overpaying on premiums with the intention to borrow against these policies later.

Stage 3: Integration through Estate Agents and Trust Companies

- **Real Estate Purchases:** The launderer contacts an estate agent (Institution 3) to buy property. The real estate acts as a legitimate asset, and the purchase is made through complex ownership structures involving shell companies established by attorneys (Institution 1) to hide the true owner.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

- **Trust Administration:** The launderer then transfers the property to a trust administered by a trust company (Institution 2). The trust company manages the property or sells it, with the proceeds appearing as legitimate income to the trust beneficiaries.

Stage 4: Further Disguise through Stock Trading and Gambling

- Stock Market Trading: Using an authorised user of an exchange (Institution 4), the launderer engages in stock market trades that appear legitimate but are designed to obscure the flow of money further. This might involve wash trades where the launderer buys and sells the same stock without realizing any significant market risk.
- Gambling: The launderer uses a portion of the funds to gamble at a licensed operator (Institution 9), buying chips, gambling minimally, and then cashing out, claiming the proceeds as gambling winnings.

Final Stage: Re-entry into the Financial System

- Loan Repayment: The launderer applies for a loan from a development finance institution (Institution 16), using the real estate as collateral. The loan proceeds are then used to repay the initial investments or insurance policies, with the launderer claiming the funds as loan proceeds, thus completing the laundering process.
- Legitimate Appearance: Through these complex transactions involving multiple accountable institutions, the illicit funds now appear as legitimate income from investments, real estate, and business activities, fully integrated into the financial system.

1.11 Targeted Financial Institutions

South Africa, as a prominent economy in Africa, operates within a complex and dynamic financial landscape. This environment necessitates robust regulatory frameworks to safeguard the integrity of its financial system, protect investors, and combat financial crimes. At the heart of these regulatory measures is the Targeted Financial Institutions List, a critical tool employed by South African regulatory authorities. This list is part of a broader strategy to identify and monitor financial institutions that pose a higher risk for activities such as money laundering, terrorist financing, and other illicit financial flows.

The Targeted Financial Institutions List is not just a regulatory measure; it serves as a linchpin in South Africa's commitment to international standards on combating financial crimes. It aligns with the recommendations of global bodies such as the Financial Action Task Force (FATF), which sets international standards for preventing money laundering and terrorist financing. By identifying institutions that require closer scrutiny, the list helps in prioritizing regulatory and supervisory efforts, ensuring that resources are efficiently allocated to areas of higher risk.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

The significance of this list extends beyond regulatory compliance. It has a profound impact on the reputation, operational capabilities, and international partnerships of the financial institutions included. Being listed can lead to enhanced due diligence from partners, potential loss of business, and, in some cases, significant legal and financial consequences. Thus, the Targeted Financial Institutions List is a critical tool for both regulators and the institutions themselves, serving as a deterrent against engaging in or inadvertently facilitating illicit financial activities.

In this section, we will explore the historical context that led to the development of the Targeted Financial Institutions List, delve into the criteria for inclusion, examine its impact on listed institutions, and provide detailed case studies to illustrate its application in real-world scenarios. Through this comprehensive analysis, readers will gain a deep understanding of the importance of the Targeted Financial Institutions List in maintaining the integrity and stability of South Africa's financial system.

1.12 Prominent Persons

The Financial Intelligence Centre Act has undergone significant amendments, specifically in the nomenclature and classification of individuals subject to scrutiny under the Act. Notably, the terms "Domestic Prominent Influential Persons" (DPIPs) and "Foreign Prominent Public Officials" (FPPOs) have been officially supplanted by "Domestic Politically Exposed Persons" (DPEPs) and "Foreign Politically Exposed Persons" (FPEPs), respectively. This change is not merely cosmetic; it aligns the Act's language with international standards on anti-money laundering and counter-terrorism financing, particularly those recommended by the Financial Action Task Force (FATF). The adjustment in terminology ensures that the Act's provisions are both current and accurately reflective of the individuals it aims to regulate. Consequently, the DocFox watchlist screening solution has updated its database to incorporate these changes, ensuring compliance and facilitating the accurate identification of individuals who may pose a financial risk.

1.12.1 Expansion of DPEP Criteria

The criteria for classifying an individual as a DPEP have been notably expanded. Previously, the Act limited the classification to individuals who had held a prominent or public position within the preceding 12 months, with an acting position lasting more than six months also qualifying. The recent amendments extend this criterion, now encompassing individuals listed in Schedule 3A, which includes Government Ministers, Executive Mayors of Municipalities, and similar positions, provided they have held such a position for a period exceeding six months, including in an acting capacity.

This expansion significantly broadens the scope of who is considered a DPEP, enhancing the Act's effectiveness in monitoring and regulating transactions that may be susceptible to corruption or money laundering.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

1.12.2 Broadening of FPEP Definition

Parallel to the adjustments made for DPEPs, the definition of an FPEP has been substantially broadened. The amendments remove the previous restriction that limited the classification to individuals who had held a prominent public position within the last 12 months. This modification means that the temporal scope for considering an individual as an FPEP is no longer capped, allowing for a more comprehensive approach in identifying and monitoring foreign individuals who, by virtue of their position, may pose a higher risk of engaging in corrupt practices or facilitating money laundering activities.

1.12.3 Introduction of Prominent Influential Persons (PIPs)

A noteworthy addition to the Act is the creation of a new category termed "Prominent Influential Persons" (PIPs), akin to the former Schedule 3A Item (b). To support this new category, Schedule 3C has been established, listing positions that qualify an individual as a PIP. These include roles such as chairpersons of the board of directors, audit committee members, executive officers, or Chief Financial Officers of companies, as defined under the Companies Act, particularly those entities that provide goods or services to an organ of state. This inclusion targets individuals in significant corporate positions, especially those involved in government contracts and tenders, underlining the Act's comprehensive approach to encompass a broader spectrum of influential roles that might influence or be susceptible to financial crimes.

These amendments mark a pivotal enhancement in the legal framework governing financial intelligence and anti-money laundering efforts. By broadening the definitions and categories of individuals subject to scrutiny, the Act aims to fortify its mechanisms for detecting and preventing financial crimes, ensuring a robust defense against corruption and the financing of terrorism within and across borders.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

Lesson 2 Compliance Obligations for Accountable Institutions

2.1 Introduction

In the complex and ever-evolving landscape of financial regulation, accountable institutions are subject to a broad spectrum of compliance obligations designed to prevent money laundering and terrorist financing. These obligations serve as the foundation for a robust regulatory framework, ensuring that institutions operate within the bounds of the law while safeguarding the financial system from illicit activities.

As we delve into this crucial aspect of financial compliance, we will explore the various obligations that accountable institutions must navigate. From implementing effective customer due diligence processes to reporting suspicious transactions and maintaining comprehensive records, each requirement plays a pivotal role in the global effort to combat financial crime. Understanding these obligations is not just a matter of legal necessity but a strategic imperative for institutions seeking to maintain operational integrity and trust in a competitive marketplace.

2.2 Registration by institutions

Accountable institutions are required to register with the FIC within 90 days from the date the business commenced with their operations.

The process of registering with the Financial Intelligence Center is essential for entities that are classified as accountable institutions. This process involves a thorough examination of the institution's business activities, customer base, and risk management strategies. In order to register with the Financial Intelligence Center, entities must submit various documentation including their business registration details, financial statements, risk assessment reports, and client identification measures.

Once submitted, the Financial Intelligence Center will assess the institution's compliance with anti-money laundering and counter-terrorism financing regulations. If the institution meets the necessary requirements, it will be granted registration and will be subject to ongoing monitoring and reporting obligations. Failure to comply with the registration process can result in severe penalties and legal action. Therefore, entities must ensure they adhere to the registration requirements set forth by the Financial Intelligence Center to avoid any potential repercussions.

After registration with the Financial Intelligence Center, individuals and entities have certain obligations and responsibilities that they must adhere to. These obligations often include conducting regular due diligence checks on clients, reporting suspicious transactions to the authorities, and keeping accurate and up-to-date records of all financial transactions.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

Additionally, those who are registered with the Financial Intelligence Center may be required to participate in ongoing training and education programs to ensure they stay informed about the latest regulations and best practices in preventing money laundering and terrorist financing. Failure to comply with these obligations can result in penalties, fines, and even legal action. Therefore, it is crucial for individuals and entities to take their responsibilities seriously and actively work towards maintaining a culture of compliance within their organizations.

2.3 Submitting Regulatory Reports

In the realm of financial compliance, accountable institutions are mandated to submit a variety of regulatory reports to the Financial Intelligence Centre (FIC) to uphold transparency and combat financial crimes effectively. This section will delve into the specifics of submitting key reports, including the Cash Threshold Report, Terrorist Property Report, Suspicious and Unusual Transaction Reports, and the International Funds Transfer Report. Each of these reports plays a crucial role in the broader effort to monitor and prevent illegal financial activities, and we will discuss the requirements and procedures for submitting these reports in the following sections.

2.3.1 Cash Threshold Report (CTR)

The obligation to report under Section 28 of the Financial Intelligence Centre Act (FIC Act) is triggered when transactions involve the payment or receipt of cash exceeding R49,999.99. This includes transactions where cash is exchanged between the accountable or reporting institution and the client, or any third party acting on behalf of either.

"Cash" is specifically defined to include coin and paper money, whether domestic or foreign, and travellers' cheques, but excludes electronic transfers and other non-physical forms of money movement.

For transactions involving foreign currency that necessitate a Cash Threshold Report (CTR), the accountable institution must convert the foreign currency to South African Rand using the exchange rate at the time of the transaction. The choice of exchange rate source is at the institution's discretion. When both cash received and paid exceed the threshold, separate CTRs for each direction of cash flow must be filed with the Centre.

The requirement to report these transactions extends to any instance where the cash component of a transaction surpasses the prescribed threshold. These reports must be submitted to the Centre within three days of the institution becoming aware of the transaction, excluding weekends and public holidays. Institutions are required to have processes in place to ensure timely reporting and should regularly review and sample reports for compliance with FIC requirements, including accurate and timely information submission according to the MLTFC Regulations.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

Particulars to be Submitted

To submit Cash Threshold Reports (CTRs) to the Financial Intelligence Centre (FIC), accountable and reporting institutions must file electronically via the FIC's internet-based portal. Before submitting CTRs, institutions need to register with the FIC to receive user credentials. This process may require institutions with multiple functions or branches to register separately for each function or location. In exceptional cases where electronic submission isn't possible, institutions must contact the FIC directly to arrange for manual report submission.

Institutions are mandated to include specific details as outlined in the Money Laundering and Terrorist Financing Control (MLTFC) Regulations.

These details can be categorized into two types: "full particulars" and "information as is readily available." Full particulars are comprehensive details that the reporting institution is expected to possess and are obligatory for report submission. On the other hand, "as much information as is readily available" pertains to details the institution may have acquired in routine operations but not explicitly verified for the purpose of the report. This distinction ensures that while comprehensive data is provided wherever possible, the reporting obligation is balanced with the practicality of information collection and availability.

When using the Centre's reporting platform, certain mandatory fields must be filled; if left blank, the report fails validation. For fields requiring "readily available" information that the reporter lacks, they should enter "not obtained." Full particulars, as per the MLTFC Regulations, must be provided when known. For example, banks and motor vehicle dealers, due to their industry practices, often have essential client information considered "readily available" for reporting. Additionally, the aggregation of cash transactions may trigger the need for both a cash threshold report and a suspicious transaction report, emphasizing the importance of monitoring and reporting as per the FIC Act's requirements.

In the context of cash threshold reporting (CTR) under the FIC Act, it's crucial to report transactions based on the directionality of the cash flow, categorizing them as either cash received or cash paid. For instance, if an accountable institution receives R50,000 in cash from a client for a product and later pays out R60,000 to the same client for the same product on the same day, both transactions must be reported separately to the Centre: one CTR for the cash received and another for the cash paid.

Recommendations to Facilitate Practical Implementation

To enhance practical implementation and compliance with reporting requirements:

- Assign unique reference numbers to clients for transactions involving another accountable institution, like a bank.
- Inform clients to use this reference number when making cash payments.
- This approach aids in accurately identifying transactions, reducing funds mistakenly held in suspense accounts.
- Link the reference number with the client upon notification of cash payments exceeding the threshold.
- Include the client's unique reference number in cash threshold reports to the Centre.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

- Banks should ensure bank statements clearly label cash transactions, as defined by the FIC Act, to assist clients in recognizing reportable cash transactions.

For example, if a client makes a cash deposit of R55,000 into their account at ABC Bank for a transaction with XYZ Motors, both institutions should use and record a unique reference number for this transaction. This number should then be included in any reports to the Centre, facilitating accurate and efficient reporting and monitoring.

2.3.2 Terrorist Property Report

Making and submitting terrorist property reports to the Financial Intelligence Center is a critical step in combating terrorism financing. These reports provide crucial information to law enforcement and intelligence agencies, enabling them to track and disrupt the flow of funds to terrorist groups.

The process of creating these reports involves thorough investigation and analysis of financial transactions, identifying suspicious patterns and connections that may be indicative of terrorist financing activities. Once a report is compiled, it must be submitted promptly to the Financial Intelligence Center, where it is further assessed and shared with relevant authorities.

Timely and accurate reporting is essential in preventing terrorist organizations from accessing the financial resources they need to carry out their violent activities. Failure to submit these reports can have serious consequences, as it may result in missed opportunities to disrupt terrorist financing networks and protect national security.

2.3.3 Suspicious and unusual transaction reports (STRs):

The purpose of the Suspicious and Unusual Transaction Reports (STRs) is to identify and report potentially illicit financial activities within the banking system. These reports are crucial in combating activities such as money laundering, terrorist financing, and other financial crimes. By requiring financial institutions to report any suspicious or unusual transactions, authorities can better monitor and investigate potential threats to the financial system.

Definition of Suspicious and Unusual Transaction Reports (STRs)

Suspicious and Unusual Transaction Reports (STRs) are defined as reports filed by financial institutions to FinCEN whenever they encounter a transaction that raises concerns regarding possible money laundering, terrorist financing, or other illicit activities. These reports are crucial in identifying and investigating suspicious activities that may not adhere to standard financial practices. STRs are essential in combating financial crimes and ensuring the integrity of the financial system.

Financial institutions are required by law to file STRs in order to report any transactions that they believe may be related to criminal activities. This helps authorities to monitor and track suspicious activities, ultimately helping to prevent money laundering and terrorist financing.STRs are a critical tool in the fight against financial crimes and play a vital role in maintaining the integrity of the global financial system.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

Importance of Reporting STRs

Reporting suspicious and unusual transaction reports (STRs) is crucial for maintaining the integrity of the financial system. By flagging questionable activities, financial institutions can help prevent money laundering, terrorism financing, and other illegal activities. Timely and accurate reporting of STRs also enables regulatory bodies to investigate and take necessary actions to safeguard the financial system from potential risks.

Additionally, sharing this information with relevant authorities allows for better coordination and collaboration in detecting and deterring financial crimes. Overall, the importance of reporting STRs cannot be understated, as it plays a vital role in maintaining the transparency and security of the financial sector.

Process of Making an STR

The process of making a Suspicious and Unusual Transaction Report (STR) is a crucial step in identifying potential instances of money laundering and terrorist financing. It begins with financial institutions monitoring customer transactions for any unusual patterns or activities that may indicate illicit behavior. Once identified, the institution then conducts a thorough investigation to gather additional information and evidence to support their suspicions. This may involve interviewing the customer, reviewing account documents, and consulting with other experts within the institution. Once all relevant information is gathered, a detailed report is prepared and submitted to the appropriate authorities, such as financial intelligence units or law enforcement agencies, for further action. The transparency and diligence of this process are essential in combating financial crime and maintaining the integrity of the financial system.

Factors Considered in Determining Suspicious Transactions

In determining suspicious transactions, several factors are taken into consideration by financial institutions and regulatory bodies. These factors include the nature and frequency of the transactions, the source of funds, the parties involved, and any unusual behavior or patterns. For example, transactions involving large amounts of cash, transfers to high-risk jurisdictions, or transactions that deviate from a customer's typical behavior may be flagged as suspicious. Additionally, transactions that are not in line with the customer's stated occupation, income level, or financial history may also trigger a suspicious transaction report. By carefully analyzing these factors, financial institutions can identify potentially illegal activities such as money laundering, terrorist financing, or fraud, and take appropriate actions to mitigate risks and comply with regulatory requirements.

Conclusion

In conclusion, suspicious and unusual transaction reports (STRs) are a vital tool in detecting and preventing financial crimes such as money laundering and terrorist financing. By requiring financial institutions to report any transactions that appear suspicious or out of the ordinary, governments and regulatory bodies can more effectively monitor and investigate potentially illicit activities. While the process of filing STRs may be time-consuming and resource-intensive for financial institutions, the benefits of identifying and stopping criminal activity far outweigh the costs. It is essential for regulators, businesses, and law enforcement agencies to work together to enhance the effectiveness of the STR reporting system and protect the integrity of the global financial system.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

2.3.4 International funds transfer reports (IFTRs)

Accountable institutions authorized to conduct cross-border transactions are mandated to report any transactions that exceed the specified threshold of R19,999.99. This requirement is part of a broader effort to enhance transparency in international financial flows and to deter illicit activities by making it more difficult for individuals or entities to move large sums of money undetected.

The reporting obligations and procedures for IFTRs are outlined in Draft Guidance Note 104A. This document serves as a comprehensive guide for accountable institutions, detailing how to accurately identify transactions that must be reported, the information that needs to be included in an IFTR, and the timelines for submission.

2.3.5 Reactive Reporting

Reactive reporting involves submitting a Suspicious Transaction Report (STR) to the Financial Intelligence Centre (FIC) in response to external prompts, despite previous suspicions based on transaction contexts. Such prompts can include subpoenas, official requests to confirm client status, intervention orders, monitoring orders, inquiries from government agencies, or adverse media information. It's crucial that these external factors, while contributing to suspicion formation, should not solely trigger an STR submission without genuine suspicion based on the transaction's specifics.

2.3.6 Legal Protection of Reporters

Under Section 38 of FICA, reporters are shielded from criminal or civil legal action for good faith compliance with reporting obligations. This protection extends to the anonymity of those reporting, prohibiting compelled testimony in criminal proceedings about the report. Disclosure of report existence or contents to others, especially the client concerned, is strictly forbidden except under specific lawful circumstances, ensuring both the reporter's safety and the integrity of the investigative process.

2.4 Implementing a Risk-based Approach

The Financial Intelligence Centre Act (FICA) underscores the importance of a risk-based approach (RBA) to effectively combat money laundering (ML), terrorist financing (TF), and proliferation financing (PF). This approach necessitates that businesses, especially accountable institutions, not only understand but also actively engage in the identification, assessment, monitoring, mitigation, and management of risks associated with these illegal activities. It's imperative for these institutions to recognize that risks vary significantly across different clients, geographic locations, products, and service offerings. The practical implementation of an RBA is pivotal in ensuring that resources are allocated efficiently and that measures taken are commensurate with the levels of risk identified. This section introduces the concept of the RBA as it pertains to FICA, with a detailed exploration provided in subsequent lessons.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

2.4.1 Understanding and Implementing the Risk-Based Approach

The implementation of an RBA under FICA involves several key steps:

- **Identification of Risks:** Accountable institutions must first identify the ML, TF, and PF risks inherent in their operations. This includes understanding how their products or services could potentially be exploited for illicit purposes.
- **Assessment of Risks:** Once risks are identified, they must be thoroughly assessed to determine their magnitude and likelihood. This assessment should consider both institutional-level and client-level risks.
- **Monitoring of Risks:** Continuous monitoring of risk factors and exposure is crucial. This allows institutions to detect changes in the risk profile and respond appropriately.
- **Mitigation and Management of Risks:** Based on the risk assessment, institutions must develop and implement strategies to mitigate identified risks. This includes adopting policies, procedures, and controls tailored to the risk level.

2.5 Developing a RMCP

Accountable institutions are required to create, document, maintain, and implement a risk management plan and compliance program tailored to their operational needs. This program is designed to ensure rigorous identity verification, proper record-keeping practices, clear criteria for reportable transactions, and adherence to prescribed guidelines by the Financial Intelligence Centre (FIC).

2.5.1 Key Components of the Program

- **Identity Verification:** Establishing protocols for confirming the identities of clients, including the collection and maintenance of relevant information.
- **Record-Keeping:** Outlining what information must be documented and the secure storage of such records.
- **Reportable Transactions:** Defining the criteria for identifying transactions that necessitate reporting, in line with FIC directives.
- **Compliance Measures:** Incorporating prescribed matters by the FIC into the institution's operations.

2.5.2 Developing the RMCP

1. **Preliminary Assessment**

Begin with a thorough assessment of your institution's exposure to money laundering and terrorist financing risks. This assessment will inform the scope and focus of your RMCP.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

2. Program Development

Craft an RMCP that includes the following key components, as mandated by FICA:

- **Establishment and Verification of Identities:** Outline procedures for identifying and verifying the identities of clients, including the use of reliable, independent source documents, data, or information.
- **Record-Keeping:** Specify the types of information to be recorded and retained, including client identification data, transaction details, and the business correspondence.
- **Determining Reportable Transactions:** Define the steps to identify transactions that must be reported to the Financial Intelligence Centre (FIC), including thresholds and indicators of suspicious activities.
- **Risk Management:** Develop strategies to identify, assess, monitor, mitigate, and manage risks associated with money laundering and terrorist financing.
- **Client Due Diligence (CDD) and Enhanced Due Diligence (EDD):** Establish processes for conducting CDD and EDD, especially for higher-risk clients, including politically exposed persons (PEPs).
- **Ongoing Monitoring and Account Review:** Implement systems for the continuous monitoring of business relationships and transactions to ensure they are consistent with the institution's knowledge of the client.
- **Compliance with Foreign Regulations:** If applicable, include measures to ensure that foreign branches and subsidiaries comply with FICA obligations and the regulations of their host countries.

2.5.3 Documentation and Approval

Document the RMCP in a comprehensive manner, detailing all procedures, responsibilities, and controls. This documentation serves as a reference for employees and a record for regulatory bodies.

The RMCP must be approved by the board of directors, senior management, or the highest level of authority within the institution. This endorsement underscores the program's significance and ensures organizational commitment.

2.6 Screening of Employees

Employee screening under the Financial Intelligence Centre Act (FICA) is a critical compliance requirement for accountable institutions. This process is designed to mitigate risks associated with money laundering (ML), terrorist financing (TF), and proliferation financing (PF) by ensuring the competence and integrity of both prospective and current employees. However, this screening must be conducted within the framework of South Africa's labour laws and the Protection of Personal Information Act (POPIA), ensuring a balanced approach between compliance and employee rights.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

2.6.1 FICA Employee Screening Requirements

Directive 8 issued by the Financial Intelligence Centre (FIC) mandates the screening of employees to assess their risk in relation to ML, TF, and PF activities. This directive, reinforced by Public Compliance Communication 55 (PCC 55), outlines the minimum standards for such screening, emphasizing the importance of a risk-based approach. Screening encompasses verifying the competence and integrity of employees, including checks against United Nations sanctions lists.

2.6.2 Balancing Compliance with Labour Laws and POPIA

The implementation of Directive 8 and PCC 55 must navigate the complexities of South Africa's labour legislation and POPIA, ensuring that employee screening does not infringe upon individual rights or violate employment laws.

Labour Laws Considerations

- **Anti-Discrimination:** Screening processes must adhere to the Employment Equity Act, avoiding discriminatory practices based on race, gender, or any other prohibited grounds.
- **Fair Procedure:** Any adverse findings from the screening process must be handled with a fair procedure in alignment with the Labour Relations Act and the Basic Conditions of Employment Act.

POPIA Compliance

- **Processing Personal Information:** Accountable institutions must ensure that the collection and processing of personal information during the screening process comply with POPIA. This includes obtaining consent where necessary and ensuring that the data collection is for a defined, lawful purpose.
- **Protection of Special Personal Information:** Details related to criminal behavior, among other sensitive information, are considered special personal information under POPIA. Institutions must have a legal basis or obtain explicit consent for processing such information.
- **Rights of Employees:** Employees have the right to be informed about the collection of their personal information and to access information about third parties who have access to their data.

2.6.3 Risk-Based Approach to Screening

- **Identifying High-Risk Roles:** Employees in positions that carry a higher risk of ML, TF, and PF—such as senior management and those in decision-making roles regarding high-risk clients—require more frequent and intensive screening.
- **Frequency of Screening:** The level of risk associated with an employee's role should determine the frequency of their screening, with high-risk positions necessitating at least annual checks.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

2.6.4 Record-Keeping and Penalties for Non-Compliance

Accountable institutions must meticulously document the screening process and maintain records of findings, ensuring they are readily accessible for FIC review.

Failure to comply with the screening requirements set forth in Directive 8 may result in substantial fines, emphasizing the importance of a diligent and compliant screening process.

2.7 Establishing Beneficial Ownership

FICA mandates that an accountable institution must establish the beneficial ownership of its clients to ensure compliance with anti-money laundering and counter-terrorism financing regulations.

Beneficial ownership refers to the natural person(s) who ultimately own or control a legal entity or arrangement. This goes beyond just knowing the named account holder or legal owner; it involves understanding who benefits from the entity's operations and assets, and who exercises control over it.

- **Application to Business Forms:** Most businesses operate in one of several forms: sole proprietorships, partnerships, companies, or trusts. Each of these has different implications for identifying beneficial ownership:
- **Sole Proprietorship:** This is the simplest form, where the business is owned and operated by a single individual. In this case, the beneficial owner is the proprietor themselves.
- **Partnership:** In a partnership, all partners may be considered beneficial owners, as they share in the profits and control of the business. The degree of beneficial ownership can vary based on the partnership agreement.
- **Company:** Identifying beneficial ownership can be more complex for companies, especially if they have a layered ownership structure with holding companies or if shares are held in nominee names. The beneficial owners are those who ultimately own a significant percentage of the shares or control the company's decisions, directly or indirectly.
- **Trusts:** For trusts, the beneficial owners are the settlor(s), the trustee(s) (to some extent), and the beneficiaries. The precise nature of beneficial ownership will depend on the trust's terms and the extent of the beneficiaries' rights.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

2.7.1 Example with Hierarchical Structure

Consider a scenario where a business is structured as follows:

- **Ultimate Beneficial Owner (UBO**): An individual who holds a controlling interest in a Holding Company.
- **Holding Company:** Owns 100% of Operating Company A and 50% of Operating Company B.
- **Operating Company A:** Engages in commercial activities under the ownership of the Holding Company.
- **Operating Company B:** Another entity partially owned by the Holding Company, with the rest owned by another entity or individual not depicted here.

In this structure, the UBO indirectly controls and benefits from the operations and assets of both Operating Companies A and B through the Holding Company. Under FICA, accountable institutions engaging with either operating company would need to identify the UBO as part of their due diligence.

Challenges and Solutions

Identifying DPEPs poses practical challenges due to the dynamic nature of political appointments and the absence of an official, comprehensive list of DPEPs in South Africa. Financial institutions often rely on self-disclosure, public records, and internet searches, which may not always yield accurate or up-to-date information.

To mitigate these challenges, some financial institutions and service providers have developed specialized databases that catalogue individuals holding positions outlined in Schedule 3A of the FIC Act. These databases are designed to streamline the identification process, reduce reliance on client disclosures, and enhance the overall efficiency of due diligence processes.

The Importance of a Risk-Based Approach

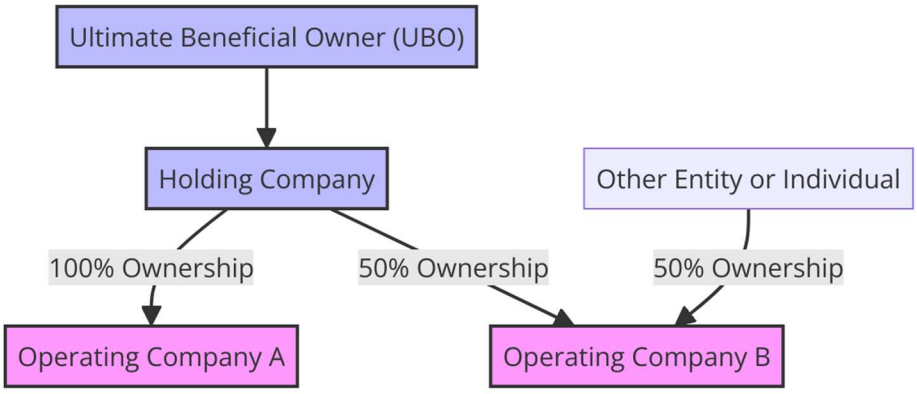
The identification of a client as a DPEP does not automatically disqualify them from doing business with financial institutions. Instead, it signals the need for a more thorough investigation into the client's financial background, particularly the origins of their funds and wealth. A risk-based approach is essential, ensuring that enhanced due diligence measures are proportionate to the level of risk associated with the DPEP.

Conclusion

The categorization of individuals as DPEPs underscores the importance of vigilance and thoroughness in the financial industry's efforts to prevent money laundering and terrorism financing. By requiring enhanced due diligence for individuals in positions of power and their close networks, South African regulations aim to safeguard the financial system against exploitation. Financial institutions must adapt to these regulatory demands, employing both technology and a risk-based approach to fulfil their compliance obligations effectively.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

Figure 2.1: Diagram indicating the Beneficial Owner



2.8 Conducting Customer Due Diligence

The Financial Intelligence Centre Act (FICA) requires certain organizations, referred to as accountable institutions, to maintain records of their business relationships and transactions. This responsibility extends to representatives associated with Financial Service Providers (FSPs).

FICA mandates that these institutions cannot start a business relationship or conduct a transaction with a client without first taking specific steps to verify the client's identity. This includes understanding who the client is and confirming their identity when they want to transact or form a business relationship. This process must align with the institution's Risk Management and Compliance Programme.

If a client is acting for someone else, the identity of both the client and the person they represent needs to be verified, including the client's authority to act on that person’s behalf. Similarly, if another person is acting for the client, their identity and authority must also be confirmed.

For existing clients from before FICA's implementation, new transactions can only occur after these identification steps are completed for all involved parties.

Institutions failing to follow these rules commit an offense.

2.8.1 Understanding and Gathering Information on Business Relationships

When starting a new business relationship, institutions must gather information to understand the nature and purpose of the relationship and the source of funds, in addition to verifying identities. This helps ensure future transactions align with what the institution knows about the client.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

2.8.2 Additional Due Diligence for Legal Entities

For clients that are legal entities (like companies or trusts), institutions need to verify identities and understand the business relationship, including the entity's business nature and its ownership and control structure.

When dealing with legal entities, it’s crucial to identify the real owners or those with significant control, either through ownership or other means like managerial roles.

2.8.3 Discontinuing Customer Due Diligence and reporting when suspicion arises

In the context of Anti-Money Laundering (AML) and Countering Financing of Terrorism (CFT) compliance, Accountable Institutions (AIs) face the critical task of conducting Customer Due Diligence (CDD). However, a complex challenge arises when the completion of CDD could potentially tip-off a client that a suspicious transaction report (STR) will be filed. The Financial Intelligence Centre Act (FICA) amendments address this scenario, providing guidance on how AIs should proceed. Additionally, the amendments introduce a new offence related to the structuring of transactions to evade reporting requirements.

1. Identifying Tipping-Off Risks

A tipping-off risk occurs when there is a suspicion or unusual activity related to money laundering (ML) or terrorist financing (TF), and completing CDD processes might inadvertently inform the client that their activities will be reported to the authorities. This situation poses a significant legal and operational challenge for AIs, as tipping off a client could obstruct justice and undermine efforts to combat financial crimes.

2. Discontinuing the CDD Process

Under the revised FICA guidelines, if an AI encounters a situation where continuing with CDD could lead to a tipping-off risk, it is permitted to halt the CDD process. This decision must be based on reasonable belief and must not be taken lightly, as it involves weighing the potential harm of tipping off against the obligation to collect full client information.

3. Reporting Suspicious Transactions

In instances where the CDD process is discontinued due to a tipping-off risk, AIs must consider filing a report in accordance with section 29 of FICA. This section mandates the reporting of suspicious or unusual transactions that may be related to ML or TF activities. The decision to file a report must be based on the AI's assessment of the risk and the suspicious nature of the transaction or client behavior.

<u>New Offence: Structuring Transactions to Evade Reporting:</u>

One of the significant amendments to FICA introduces a new offence related to the structuring of transactions. This offence occurs when an AI deliberately structures transactions in a manner that avoids triggering reporting obligations. The aim of such structuring could be to stay below threshold amounts that necessitate reporting or to avoid drawing attention to the transaction's suspicious nature. This amendment underscores the regulatory emphasis on ensuring that AIs do not engage in practices that could facilitate financial crimes by evading detection and reporting mechanisms.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

2.8.4 Ongoing Due Diligence

Institutions must continuously monitor their business relationships, including transaction sources and purposes, to ensure consistency with the client's profile and to keep client information up to date.

2.8.5 Doubts About Previously Obtained Information

If there are doubts about the accuracy of previously verified information, institutions must re-verify this information as necessary.

2.8.6 Dealing with Foreign Prominent Public Officials

Special attention is required when the client or their owner is a foreign prominent public official. Approval from senior management, understanding the source of their wealth, and enhanced monitoring are needed.

2.8.7 Inability to Conduct Customer Due Diligence

If an institution cannot verify a client's identity or obtain necessary information, it must not start or must terminate the business relationship, possibly reporting the client under FICA's regulations.

2.8.8 Single Transaction Threshold

FICA sets a threshold for single transactions, which are not part of an ongoing business relationship, at R5,000. Transactions below this amount are considered occasional and do not require full due diligence, except in cases where transactions involve anonymous clients or those with suspicious identities, where some level of identification is still needed.

2.9 Scrutinise Clients Against Financial Sanctions List

The Financial Intelligence Centre (FIC) is tasked with administering the targeted financial sanctions (TFS) set forth by the United Nations Security Council (UNSC) resolutions. These sanctions, aimed at combating the proliferation of weapons of mass destruction, require member states to enforce restrictions on specified individuals, entities, countries, goods, and services. Such measures include denying access to funds and financial services for those identified under TFS.

To implement these sanctions, the Minister of Finance publishes notices in the Government Gazette upon adoption of UNSC resolutions, while the FIC Director identifies sanctioned individuals or entities. These notices are binding until revoked and prohibit transactions with or the provision of financial services to sanctioned parties, maintaining the status quo of their assets at the time of sanction.

Accountable institutions must freeze assets related to sanctioned parties and report such holdings to the FIC. They are also responsible for screening clients against the sanctions list to ensure compliance, recognizing that non-compliance constitutes a criminal offense.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

Additionally, the Minister of Finance can authorize exceptions for basic living expenses or necessary business activities under specific conditions, communicated through written permissions and published by the FIC. This framework ensures adherence to international obligations while maintaining national security and financial system integrity.

2.10 Determine Status of Person

Accountable Institutions (AIs) face the crucial responsibility of identifying the nature of their clientele, especially in distinguishing Politically Exposed Persons (PEPs) and Domestic Prominent Influential Persons (DPIPs). This identification process is foundational to implementing enhanced due diligence measures. Public Compliance Communication 51 (PCC 51) provides detailed guidance on this matter, emphasizing the importance of understanding the status of clients to ensure compliance with the Financial Intelligence Centre (FIC) Act.

2.10.1 Definitions and Categories

- **Foreign Politically Exposed Persons (Foreign PEPs):** Individuals who are or have been entrusted with prominent public functions by a foreign country, including heads of state or government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, and important political party officials.
- **Domestic Politically Exposed Persons (Domestic PEPs):** Individuals within the same categories as foreign PEPs but are entrusted with prominent public functions domestically.
- **Domestic Prominent Influential Persons (DPIPs):** Individuals who hold significant positions within the private sector or within organizations that have a major role in domestic politics and society, but who do not fit the traditional definition of a PEP.

2.10.2 Compliance Requirements

1. Identification and Verification

AIs must establish processes to identify whether a client, or a potential client, falls into one of these categories. This involves not only initial verification upon establishing a business relationship but also ongoing monitoring to capture any change in the client's status.

2. Enhanced Due Diligence (EDD)

Clients identified as PEPs or DPIPs require EDD measures, which go beyond standard due diligence practices. EDD measures may include obtaining additional information on the source of funds or wealth, the intended nature of the business relationship, and obtaining senior management approval for establishing or continuing such relationships.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

3. Risk Management

The identification of a client as a PEP or DPIP inherently suggests a higher risk of money laundering or terrorist financing. AIs are expected to manage these risks by implementing appropriate risk management systems and controls as outlined in the FIC Act and further detailed in PCC 51.

4. Ongoing Monitoring

Continuous monitoring of transactions and business relationships with PEPs and DPIPs is essential to detect suspicious activities and ensure compliance over time. This includes keeping client profiles up to date and regularly reviewing the adequacy of EDD measures.

2.10.3 Regulatory Guidance: PCC 51

PCC 51 serves as a cornerstone for AIs in understanding the requirements for dealing with PEPs and DPIPs. It outlines the procedures for identifying such individuals, the kinds of information and documentation that should be collected, and the strategies for assessing associated risks.

2.11 Monitor Transaction

Transaction monitoring represents a crucial component of an accountable institution's compliance and risk management practices. It involves the diligent examination of individual transactions as well as the aggregate activity over the duration of a business relationship with a client. The core objective is to ensure that these transactions are consistent with the institution's understanding of the client's profile, including their business activities and risk exposure to money laundering (ML), terrorist financing (TF), and proliferation financing (PF).

The primary purpose of transaction monitoring is twofold:

- **Identifying Suspicious and Unusual Transactions:** By continuously analyzing transaction patterns and comparing them against established norms of the client's financial behavior, institutions can detect anomalies. These anomalies may suggest that a transaction or series of transactions do not align with what would be expected based on the client's known activities, financial history, or risk profile. Such discrepancies could indicate potential ML, TF, or PF activities, necessitating further investigation.
- **Detecting Large Cash Payments:** In addition to identifying suspicious activities, transaction monitoring systems are designed to flag large cash transactions. Given the higher risks associated with cash in facilitating anonymity in financial dealings, such transactions are subject to stricter scrutiny to ensure they are not part of attempts to launder money, finance terrorism, or support proliferation activities.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

Transaction monitoring employs sophisticated algorithms and analytical processes within financial systems to scrutinize transaction data in real-time or on a batch processing basis. These systems are configured to flag transactions that meet predefined criteria indicating potential risk, such as:

- Transactions exceeding certain monetary thresholds.
- Transactions to or from high-risk jurisdictions.
- Rapid movement of funds between accounts without a clear business rationale.
- Transactions that do not fit the typical pattern of activity for the client or the sector in which they operate.

Upon flagging a transaction, the system alerts compliance officers or designated personnel within the institution, who then undertake a more detailed analysis to determine the nature of the transaction. This may involve reviewing the context of the transaction, the parties involved, and any documentation supporting the transaction's purpose.

Should a transaction be deemed suspicious following a review, accountable institutions are obligated to report this to the relevant financial intelligence or regulatory bodies as per the legal and regulatory framework governing ML, TF, and PF within their jurisdiction. This reporting plays a critical role in the broader efforts to combat financial crimes and maintain the integrity of the financial system.

2.11.1 The Automated Transaction Monitoring Systems (ATMS) Directive

The purpose of this Directive is to establish guidelines for the use of Automated Transaction Monitoring Systems (ATMS) by reporting entities. It aims to ensure the identification of potentially suspicious and unusual transactions or patterns of transactions through ATMS, while maintaining proper governance structures to adhere to all reporting obligations effectively.

The requirements of the directive are as follows:

- **Immediate Attention to Alerts:** Entities that have implemented ATMS are required to address all generated alerts within 48 hours to determine if a report should be made to the Financial Intelligence Centre (FIC).
- **Acknowledgment of Suspicious Activity**: Upon the generation of an alert by the ATMS, the reporting entity is considered to have knowledge of potential suspicious or unusual activity.
- **Timely Reporting:** Reports on suspicious or unusual transactions or activities must be submitted to the FIC as stipulated in regulation 24(3), no later than 15 days after the alert generation by the ATMS.
- **Adherence to ATMS Usage Conditions:** Entities are mandated to comply with specific conditions for utilizing an ATMS, outlined in the subsequent section.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

Entities must ensure the following to comply with ATMS usage requirements for effective risk management against money laundering and terrorist financing:

- **Governance and Oversight:** The entity's board of directors or senior management must oversee the ATMS implementation, including alert management, rule adequacy, and reporting processes.
- **Alert Investigation:** All alerts must be promptly investigated to ensure timely reporting to the FIC.
- **Responsibility Allocation:** Clear responsibilities must be assigned within the organization for the review, investigation, and reporting of ATMS-generated alerts.
- **Staff Competency:** Individuals responsible for handling alerts must possess the necessary skills and receive regular training to identify suspicious activities.
- **Documentation:** Investigations and decisions regarding alerts must be well-documented and accessible for review by supervisory bodies or the FIC.
- **Resource Allocation:** Adequate resources must be allocated to manage the volume of alerts and prevent backlogs.
- **Detection Rule Development:** Should a suspicious activity be detected outside the ATMS, detection rules must be developed to capture similar activities in the future.
- **Manual Reporting:** The use of an ATMS does not exempt entities from processing manual reports of suspicious activities.
- **Methodology Validation:** The detection methodology of the ATMS must be regularly validated and tested to ensure effectiveness.
- **RMCP Inclusion:** The process for reporting and investigating automated alerts must be incorporated into the entity's Risk Management and Compliance Programme (RMCP).
- **Annual Review**: The effectiveness of the ATMS should be reviewed and approved annually by the highest level of authority within the entity.
- **Ongoing Risk Assessment:** The ATMS must undergo continuous risk assessment and tuning to remain effective.
- **Governance of Configuration Changes:** Any changes to the ATMS must follow a documented procedure and be authorized by senior management before implementation.
- **Audit Trail Maintenance:** A clear audit trail of all changes and configurations to the ATMS must be maintained.
- **Methodology Documentation:** The detection methodology used by the ATMS must be clearly documented and included in the entity's RMCP.
- **Customization for Domestic Risks:** For entities that are part of international organizations using ATMS, the system must be customized to address domestic risks adequately.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

- **Holistic Monitoring:** Entities must ensure that the ATMS monitors clients and transactions across all services, including those conducted by agents.
- **Integration of Multiple ATMS:** If multiple ATMS are used, entities must ensure they provide a comprehensive view of all alerts and reports for each client.
- **Availability of Evaluation Reports**: Upon request, entities must provide reports on the ATMS evaluation to the FIC or relevant supervisory body.

Failure to adhere to the Directive may lead to administrative sanctions as per section 45C of the FIC Act, underscoring the importance of compliance with these requirements.

2.12 Keeping Records

Accountable institutions are mandated to adhere to specific record-keeping practices as part of their compliance with the Financial Intelligence Centre Act (FIC Act). These practices are crucial for maintaining a transparent record of client interactions, transactions, and regulatory compliance efforts. This section outlines the statutory requirements for record retention, the format of record storage, and principles to ensure the accessibility and integrity of these records.

2.12.1 Record Retention Periods

The FIC Act stipulates distinct retention periods for various categories of records:

- **Client Identification and Verification Records:** Must be retained for a period of five years following the end of the business relationship with the client.
- **Transactional Information**: Should be kept for five years from the date on which a transaction is completed.
- **Regulatory Reports:** Any reports submitted to the Financial Intelligence Centre, as required under section 29 of the FIC Act, need to be preserved for five years from the date of submission.

2.12.2 Format of Record Storage

Records may be preserved in electronic form, which offers flexibility and efficiency in storage and retrieval processes. However, regardless of the storage method, certain principles must be universally applied to safeguard the accessibility and integrity of these records:

- **Accessibility:** Accountable institutions must ensure they have free and unimpeded access to all required records. This principle supports the timely review and analysis of information for compliance and reporting purposes.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

- **Availability:** Records must be readily available to the Financial Intelligence Centre and the relevant supervisory body upon request. This availability is critical for regulatory examinations, audits, and investigations.
- **Legibility:** All records, whether stored electronically or in physical form, must be capable of being reproduced in a legible and comprehensible format. This ensures that the information can be effectively reviewed and analyzed by both the institution and regulatory authorities.
- **Off-Site Storage Considerations:** If records are stored off-site, whether by a third-party service provider or in a remote storage facility, the institution must provide the Centre and the supervisory body with detailed information about the storage location and the entity responsible for the records. This transparency facilitates regulatory access to records, even when they are not housed within the institution's primary premises.

2.13 Appointing Compliance Officer

In the framework of the Financial Intelligence Centre Act (FIC Act), establishing a compliance function is a fundamental requirement for accountable institutions. This function is designed to aid the board of directors or senior management in fulfilling their legal and regulatory obligations. Central to this function is the appointment of a compliance officer—a role that carries significant responsibility for ensuring the institution's adherence to the FIC Act and its internal Risk Management and Compliance Programme (RMCP).

2.13.1 Role and Responsibilities of the Compliance Officer

The compliance officer acts as the linchpin in the institution's efforts to combat money laundering (ML) and terrorist financing (TF). This individual's responsibilities include:

- **Overseeing the Compliance Function:** Implementing and managing the institution's compliance strategies and policies.
- **Advisory Role:** Providing guidance to the board of directors, senior management, and employees on compliance matters to ensure understanding and adherence to the FIC Act and RMCP.
- **Training and Awareness**: Developing and delivering training programs to ensure that all staff are aware of their compliance responsibilities.
- **Monitoring and Reporting:** Regularly reviewing and assessing the institution's compliance with legal obligations, and reporting on compliance matters to the senior management and relevant regulatory bodies.
- **Liaison with Regulatory Bodies:** Acting as the primary contact point for communication with regulatory authorities on compliance and reporting issues.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

2.13.2 Competence and Seniority

The effectiveness of the compliance function hinges on appointing a compliance officer with the requisite competence, seniority, and authority. The appointed individual must possess:

- **In-depth Knowledge:** A comprehensive understanding of the FIC Act, associated regulations, and the specific compliance risks facing the institution.
- **Leadership Qualities:** The ability to influence and drive compliance culture across the institution.
- **Decision-Making Capacity:** Sufficient seniority to make impactful decisions regarding the institution's compliance policies and procedures.

2.13.3 Governance Structure and Compliance

For institutions with a formal governance structure, such as a board of directors, it is crucial to ensure that the compliance officer has the support and resources needed to enforce compliance effectively. In institutions without a formal governance structure, senior management must fulfill this role, ensuring that compliance obligations are met.

In cases where the accountable institution is not recognized as a legal person (excluding sole proprietors), it remains imperative to designate competent individual(s) to support the highest level of authority in meeting compliance obligations.

2.13.4 Accountability and Assistance

While accountable institutions may seek external assistance for certain compliance functions, the ultimate responsibility for compliance with the FIC Act rests with the institution itself. Institutions must ensure that sensitive information, particularly related to suspicious and unusual transaction reports, is handled securely and that passwords and other secure information are not shared.

2.14 Employee Training

Under the Financial Intelligence Centre Act (FIC Act), accountable institutions are obligated to conduct employee training. While the Act does not prescribe a specific format for this training, the Financial Intelligence Centre (the Centre) emphasizes that the training should be comprehensive enough to ensure employees can adhere to the provisions of the FIC Act as well as the institution's Risk Management and Compliance Programme (RMCP). This section delves into the objectives, content, and suggested methodologies for effective FICA training within accountable institutions.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

The primary goal of FICA employee training is to equip staff with the knowledge and skills necessary to effectively contribute to the institution's compliance efforts. Specifically, training aims to:

- Enhance awareness of the legal obligations under the FIC Act.
- Familiarize employees with the institution's RMCP, including policies, procedures, and controls put in place to mitigate money laundering (ML) and terrorist financing (TF) risks.
- Enable employees to identify and report suspicious transactions or activities in accordance with the FIC Act and internal protocols.
- Foster a compliance culture within the institution that values ethical conduct and adherence to regulatory requirements.

2.14.1 Content of FICA Training Programs

Effective FICA training programs should cover a broad range of topics related to AML and CFT compliance, including but not limited to:

- An overview of the FIC Act and its implications for the institution and its employees.
- The concept of money laundering and terrorist financing, including common methods and indicators.
- Detailed examination of the institution's RMCP, highlighting employee roles and responsibilities in supporting compliance.
- Procedures for conducting customer due diligence (CDD) and enhanced due diligence (EDD) where applicable.
- Guidelines for identifying and reporting suspicious transactions or activities to designated internal units or directly to the Centre.
- Updates on emerging trends in ML and TF, including new typologies and regulatory amendments.

2.14.2 Methodologies for Delivering FICA Training

While the FIC Act does not mandate a specific training format, accountable institutions are encouraged to adopt a flexible and engaging approach to training delivery. Possible methodologies include:

- **Classroom Training:** Traditional in-person sessions that facilitate interaction and discussion among participants and trainers.
- **E-Learning Modules:** Online training programs that allow employees to complete courses at their own pace, ideally supplemented with quizzes or assessments to gauge comprehension.
- **Workshops and Seminars:** Interactive sessions focused on practical aspects of compliance, including case studies and scenario analyses.
- **Regular Updates and Bulletins**: Ongoing communications that keep employees informed about new developments, regulatory changes, and emerging risks in AML and CFT.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

Lesson 3 Practical Implementation of FICA Framework

3.1 Introduction

In today's dynamic business world, staying ahead means constantly refining financial management practices. Enter the Financial Capability Assessment Framework (FICA) – your blueprint for financial finesse. This framework isn't just a tool; it's a game-changer, offering a step-by-step strategy to elevate your organization's financial health. As we dive into the nuts and bolts of FICA, we'll uncover the essentials, perks, and hurdles of integrating this powerhouse into your operations. Ready to boost your financial prowess and propel your organization toward enduring prosperity? Let's break down how FICA can be your financial compass in the journey to business excellence.

3.2 Understanding the FICA Framework

Alright, let's get practical with a dash of sass and a sprinkle of motivation! Implementing the FICA framework isn't just a regulatory must-do; it's your chance to shine as a compliance superstar. Here's how you're going to rock it:

- **Directors, take charge!** It's on you to ensure the FICA framework is more than just paperwork. Dive into the Financial Intelligence Centre Act, and don't just skim it—own it.
- **Appoint a FICA Compliance Officer:** This person is your right hand, the master of details, ensuring that the day-to-day compliance tasks are on point. Make it official in your Compliance Charter because, hey, if it's not written down, did it even happen?
- **Teamwork makes the dream work:** Gather your board of directors, your newly minted compliance officer, and groups of savvy employees to craft a Risk Management and Compliance Program that's so good, it practically glows.
- **Culture is key:** Every employee, from the mailroom to the boardroom, needs to live and breathe FICA in their daily duties. Make compliance a part of your corporate DNA.

Remember, implementing FICA is not just about avoiding penalties; it's about protecting your organization's integrity and contributing to the global fight against financial crime. Let's get compliant!

To combat the grey listing's implications, South Africa has initiated several actions, including legislative amendments and the establishment of the Fusion Centre to consolidate efforts against financial crimes. These measures reflect a broad commitment across government and financial authorities to address the FATF's concerns and strengthen South Africa's financial integrity on the global stage.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

3.3 Importance of Implementing FICA within Organizations

By adhering to FICA regulations, organizations can protect themselves from legal and reputational risks that may arise from non-compliance. Additionally, implementing FICA within an organization can also improve transparency and accountability, as it requires companies to conduct due diligence on their customers and establish robust internal controls. Failure to adhere to FICA regulations can result in hefty fines, damaged reputations, and loss of trust from stakeholders.

Implementing FICA is vital for organizations to combat financial crimes like money laundering and terrorist financing. Adherence to FICA not only mitigates legal and reputational risks but also enhances transparency and accountability by mandating customer due diligence and robust internal controls. Non-compliance could lead to significant fines, reputational damage, and loss of stakeholder trust. Thus, prioritizing FICA's implementation is crucial for maintaining ethical standards and safeguarding operations within the financial sector.

REAL LIFE EXAMPLE
South African Greylisting

The Financial Action Task Force (FATF) placed South Africa on its grey list in February 2023, marking a significant moment for the nation's financial sector. This grey listing signifies that South Africa is under increased scrutiny due to deficiencies in its anti-money laundering (AML) and combating the financing of terrorism (CFT) frameworks. The country has committed to addressing these deficiencies by January 2025, showcasing a national effort to strengthen its financial regulatory environment.

The grey list is not intended as a punitive measure but rather aims to motivate and support countries in enhancing their AML/CFT systems. Being on this list means South Africa faces increased monitoring by the FATF and will likely undergo heightened due diligence checks by international partners, potentially affecting cross-border financial transactions and international trade relations.

South Africa's grey listing is attributed to various strategic deficiencies, including the need for better risk-based supervision of non-financial businesses and professions, enhanced access to accurate and up-to-date beneficial ownership information, and stronger enforcement of AML/CFT laws. Additionally, the country is expected to demonstrate improvements in the investigation and prosecution of serious money laundering and terrorism financing activities, aligning with its risk profile.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

3.3.1 Grey Listing Implications

To combat the grey listing's implications, South Africa has initiated several actions, including legislative amendments and the establishment of the Fusion Centre to consolidate efforts against financial crimes. These measures reflect a broad commitment across government and financial authorities to address the FATF's concerns and strengthen South Africa's financial integrity on the global stage.

The practical impact of the grey listing includes potential challenges for South African entities engaging in international transactions, as foreign counterparts might apply enhanced scrutiny. However, the National Treasury and financial regulatory bodies like the Financial Sector Conduct Authority (FSCA) and the South African Reserve Bank (SARB) have emphasized their commitment to ensuring limited impacts on financial stability and the cost of doing business with South Africa. They are focused on enhancing AML/CFT compliance and encouraging accountable institutions to increase their vigilance and reporting of suspicious transactions.

In addressing the FATF's concerns, South Africa is not only working to be removed from the grey list but also to fortify its financial system against money laundering and terrorism financing risks, setting a precedent for continuous improvement in financial regulation and oversight.

For detailed insights into South Africa's grey listing and the actions being taken, refer to the comprehensive analysis provided by Bowmans, Investec, and Cliffe Dekker Hofmeyr.

3.4 Risk-Based Approach in FICA Implementation

The Risk-Based Approach (RBA) to Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) is a method that requires financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess, and understand the money laundering (ML) and terrorist financing (TF) risks to which they are exposed and to take appropriate measures to mitigate these risks. This approach is fundamentally about allocating resources in a manner that prioritizes and addresses the most significant risks, which is considered more effective and efficient compared to a one-size-fits-all or checklist approach.

RBA Differs from Other Approaches in the following manners:

1. **Risk Identification and Assessment**: Unlike prescriptive approaches that dictate specific controls for all entities regardless of their risk exposure, RBA starts with a thorough risk assessment process. Entities must identify and evaluate the risks specific to their operations, customers, geographical locations, products, and services.
2. **Tailored Controls**: Based on the risk assessment, institutions develop and implement controls that are proportionate to the nature and level of risks identified. This means that higher-risk areas receive more attention and resources, while lower-risk areas are managed accordingly, optimizing the use of resources.
3. **Flexibility and Dynamism**: RBA allows for flexibility and adaptation over time. As risks evolve, so too can the institution's control measures. This contrasts with static approaches where changes in risks may not be as swiftly reflected in the controls.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

4. **Enhanced Due Diligence (EDD)**: For higher-risk customers, RBA mandates enhanced due diligence measures to mitigate the identified risks effectively. This is in contrast to a uniform approach where the same level of due diligence might be applied to all customers, regardless of risk.
5. **Continuous Monitoring and Review**: An RBA requires ongoing monitoring and periodic review of both the risk environment and the effectiveness of controls implemented. Other approaches might not necessitate such continuous adaptation or reassessment.

3.5 Identify the Risks

In the complex and ever-evolving landscape of Anti-Money Laundering and Terrorist Financing (AML/TF), adopting a risk-based approach is crucial for financial institutions and other obligated entities. This approach begins with a thorough identification of the myriad types of risks that an organization might face. Such risks are not uniform but vary widely depending on numerous factors, including the nature of the business, its customer base, the products and services it offers, and the geographies within which it operates. Understanding and categorizing these risks is the first step towards developing effective strategies to mitigate them. Key areas of focus include customer risk, which examines the potential AML/TF threats posed by different types of customers; product and service risk, which assesses how certain offerings might be exploited for illicit purposes; geographical risk, which considers the challenges posed by operating in or dealing with certain jurisdictions; and delivery channel risk, which looks at the vulnerabilities inherent in the various methods through which products and services are delivered. By starting with a clear identification of these risk categories, organizations can tailor their AML/TF compliance programs to address specific vulnerabilities, thereby enhancing their overall risk management framework.

3.5.1 Customer Risk

Consider the background, nature, and behavior of your customers. High-risk customers might include politically exposed persons (PEPs) or entities from jurisdictions with weak AML/CFT controls. Here are key indicators that Financial Service Providers (FSPs) and learners can use to identify customer risk:

1. **Customer Profile**
    - Occupation or business activities that are cash-intensive.
    - Ownership structure of corporate clients that is unnecessarily complex.
    - Use of intermediaries to obscure ownership or control.
2. **Geographic Location**
    - Residency or operations in countries known for high levels of corruption, inadequate AML/TF controls, or high-risk activities (e.g., drug trafficking, smuggling).
    - Frequent transactions involving high-risk jurisdictions.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

3. **Transaction Patterns**
    - Unusual transaction patterns that do not fit the customer's profile or business activities.
    - High volume of transactions in a short period, especially in cash.
    - Frequent cross-border transactions without a clear economic purpose.
4. **Banking Habits**
    - Reluctance to provide complete information or providing inconsistent information over time.
    - Use of anonymous products (e.g., prepaid cards) or services that provide a high degree of anonymity.
    - Rapid movement of funds to and from the account without a clear business reason.
5. **Products and Services Used**
    - Interest in or use of products that are complex, unusually risky, or designed for anonymity.
    - Utilization of products or services that facilitate rapid international fund transfers without clear business reasons.
6. **Source of Funds or Wealth**
    - Difficulty in determining the legitimate source of funds or wealth.
    - Funds originating from or sent to entities or individuals associated with criminal activities or sanctioned entities.
7. **Political Exposure**
    - Customers who are politically exposed persons (PEPs), their family members, or close associates, especially from countries with high corruption levels.
8. **Adverse Media**
    - Negative news or reports about the customer or their associates related to financial crimes, corruption, or other illicit activities.

3.5.2 Product and Service Risk

Some products or services might be more susceptible to misuse for money laundering, such as those allowing for anonymity or rapid movement of funds across borders. These indicators help in assessing the potential for products and services to be misused for money laundering or terrorist financing purposes:

- **Anonymity:** Products or services that allow transactions without revealing the identity of the user (e.g., prepaid cards, online wallets).
- **Cross-Border Transactions:** Services facilitating cross-border transfers without adequate monitoring or controls, increasing the risk of funds being moved to high-risk jurisdictions.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

- **Payment Methods:** Products allowing the use of cash or third-party transfers, which can obscure the origin of funds.
- **High-Value Transactions:** Services that involve high-value transactions or large volumes of transactions, which may not align with the customer's profile.
- **Complexity and Lack of Transparency:** Complex products or services with opaque structures that make it difficult to understand the flow of funds.
- **New Products and Technologies:** Innovative financial products or the use of new technologies (e.g., cryptocurrencies, blockchain) that may not yet be fully regulated or understood.
- **Private Banking:** Services offering a high degree of privacy to customers, which could be exploited to hide the ownership of funds.
- **Correspondent Banking:** Banking services provided to foreign financial institutions, which might be used to bypass local AML/TF controls.
- **Investment and Securities:** Products related to investments or securities that can be used to layer illicit funds within legitimate financial systems.
- **Wire Transfers:** Services that enable rapid and potentially untraceable wire transfers, especially to and from countries with inadequate AML/TF measures.
- **Non-Face-To-Face Business Relationships:** Products or services set up or conducted without in-person verification, increasing the risk of identity fraud.
- **Cash Intensive Businesses:** Services used by businesses that handle large amounts of cash, which can easily be mingled with illicit funds.

3.5.3 Geographical Risk

Assess the risk posed by operating in or dealing with countries known for high levels of corruption, inadequate AML/CFT measures, or sanctions. These indicators help in identifying the risk level associated with specific geographic areas, influencing the level of due diligence and monitoring required:

- **High-Risk Countries:** Countries identified by credible sources (e.g., FATF, EU, OFAC) as having significant deficiencies in their AML/TF regimes or being non-cooperative in international efforts to combat money laundering and terrorist financing.
- **Countries Subject to Sanctions, Embargoes, or Similar Measures:** Jurisdictions that are the target of sanctions, embargoes, or related measures imposed by international bodies or countries, indicating higher risks of financial crime.
- **Countries with High Levels of Corruption or Crime:** Jurisdictions known for high levels of corruption, organized crime, drug production, or trafficking, as these environments can foster money laundering activities.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

- **Offshore Financial Centers:** Countries or territories that offer financial services to non-residents on a scale that is incommensurate with the size and the financing of their domestic economies, often with enhanced secrecy and low taxation.
- **Countries with Weak Regulatory Systems:** Jurisdictions with inadequate regulatory frameworks or poor enforcement of AML/TF laws and regulations, making them vulnerable to financial crime.
- **Conflict Zones:** Areas experiencing conflict, including countries, regions, or territories, where the breakdown of governance and the presence of armed groups can lead to increased risk of terrorist financing.
- **Jurisdictions with Secrecy Laws:** Countries that provide strict banking secrecy, hindering transparency and the exchange of information for AML/TF purposes.
- **High-Risk Third Countries:** Jurisdictions with strategic deficiencies in their AML/TF framework that pose significant threats to the international financial system.

3.5.4 Delivery Channel Risk

Digital and non-face-to-face channels might carry higher risks due to the challenges in verifying customer identities. It's important to identify the specific ways through which products and services are delivered that might elevate the institution's exposure to money laundering or terrorist financing risks. Here's a comprehensive list:

- **Non-Face-to-Face Business Relationships and Transactions:** Services that do not require physical presence for customer identification and verification, which may increase the risk of identity fraud or impersonation.
- **Internet-Based Services:** Online banking, digital wallets, and other internet-based financial services that might allow for anonymity or make it difficult to trace transactions and verify identities.
- **Mobile Banking and Payments**: Services provided through mobile devices that could potentially bypass traditional controls and customer due diligence measures.
- **Third-Party Payment Service Providers:** Use of external entities to process payments, which might introduce additional layers of separation between the financial institution and the customer, complicating the monitoring of transactions.
- **Wire Transfers:** The ability to quickly move funds internationally through wire transfers, which can be used to obscure the origin and destination of illicit funds.
- **ATM Transactions**: High-volume or high-value transactions conducted through ATMs, especially withdrawals or deposits, that may not be directly monitored in real-time.
- **Correspondent Banking:** Relationships with other banks to provide services in jurisdictions where the institution does not have a physical presence, potentially exposing the institution to the risks associated with the correspondent bank's own AML/TF controls.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

- **New Payment Products and Technologies:** Introduction of new payment methods (e.g., cryptocurrencies, blockchain technology) that might not fully fall under existing regulatory frameworks or whose risk profiles are not yet fully understood.
- **Agent or Third-party Operated Services:** Services where the institution relies on agents or third parties to conduct customer due diligence or transaction monitoring on its behalf, which may lead to inconsistencies or lapses in AML/TF controls.

3.5.5 Practical Example: Sarah identifies risks

In the heart of the bustling financial district, Sarah, a FICA compliance officer with an eye for detail and a knack for investigation embarks on a critical mission. Tasked with safeguarding "Secure Futures Inc.," a reputable financial institution, Sarah must navigate through the complex world of Anti-Money Laundering (AML) and Terrorist Financing (TF) to identify potential risks. Drawing inspiration from her detective-like diligence and analytical prowess, let's explore how Sarah approaches this challenge.

Steps to Identify AML/TF Risks

1. **Deep Dive into Business Operations:** Sarah starts by dissecting the operational framework of Secure Futures Inc., scrutinizing the variety of financial products and services they offer. Her goal is to understand the mechanisms through which these offerings might be manipulated for illicit purposes.
2. **Customer Base Evaluation:** With her magnifying glass in hand, Sarah meticulously examines the institution's clientele. She categorizes customers based on their risk profile, paying special attention to those with political connections (PEPs), individuals from countries with lax AML/TF measures, and entities operating in sectors prone to financial crimes.
3. **Geographical Risk Assessment:** Sarah maps out the global footprint of Secure Futures Inc.'s customer base. She highlights regions with notorious reputations for corruption or political instability and gauges the impact on the institution's exposure to AML/TF risks.
4. **Product and Service Scrutiny:** Analyzing the financial products in detail, Sarah identifies features that could potentially be attractive to money launderers or terrorist financiers. She zeroes in on products that allow for anonymity, offer investment opportunities, or have flexible cash surrender policies.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

5. **Transaction Behavior Analysis:** With her pipe thoughtfully positioned, Sarah delves into transaction patterns and payment methods. She looks for anomalies such as overpayments, frequent beneficiary changes, or an unusual reliance on cash transactions, which could signal attempts to launder money.
6. **Regulatory Landscape Review:** Sarah updates her knowledge on the latest AML/TF regulations affecting financial institutions. She ensures that Secure Futures Inc.'s compliance frameworks are robust and in line with current legal requirements.
7. **Intermediary and Channel Oversight:** Finally, Sarah evaluates the network of third-party agents and digital platforms Secure Futures Inc. uses to reach and serve its clients. She assesses the risks associated with these indirect channels, particularly focusing on the challenges of maintaining direct oversight and enforcing compliance standards.

Identified AML/TF Risks

Through her thorough investigation, Sarah uncovers several key areas of concern for Secure Futures Inc.:

1. **High-risk Customers:** Individuals with political influence or those hailing from jurisdictions with weak AML/TF controls pose a significant risk.
2. **Vulnerable Products:** Certain financial offerings, especially those providing anonymity or investment opportunities, are prone to misuse.
3. **Cash-based Transactions:** The institution's acceptance of cash payments for certain services increases its susceptibility to money laundering activities.
4. **Anomalous Transactions:** Patterns such as overpayment or erratic changes in policy details suggest potential laundering or financing of terrorism.
5. **Reliance on Third-party Intermediaries:** The use of external agents without stringent compliance checks introduces additional risk layers.
6. **Digital Channels:** The growth in online transactions without adequate identity verification processes elevates the risk of fraudulent activities.

Like a true detective, Sarah's methodical approach to identifying AML/TF risks at Secure Futures Inc. is a testament to the importance of vigilance and precision in the financial sector's battle against money laundering and terrorist financing. By leveraging her unique blend of traditional detective skills and modern compliance knowledge, Sarah ensures that Secure Futures Inc. remains a step ahead in maintaining a secure and trustworthy financial environment.

3.6 Create Risk Matrix

To effectively manage and assess risks, particularly in the field of Anti-Money Laundering (AML) and Terrorist Financing (TF), understanding and applying a risk matrix is crucial. This tool helps in visualizing and determining the level of risk associated with specific activities or decisions. Here's a clearer explanation, broken down into sections for better understanding:

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

3.6.1 What is a Risk Matrix?

A risk matrix is a visual tool used in risk management to assess the severity of potential risks by considering two main factors: the likelihood of an event occurring and its potential impact. This matrix helps organizations prioritize risks and allocate resources more efficiently to mitigate them.

3.6.2 Understanding the Axes

- **Likelihood Axis**: This axis measures the probability that a risk event will occur. In the context of AML/TF, it evaluates how likely it is for an institution to be used for money laundering or terrorist financing. The scale typically ranges from low to high.
- **Impact Axis**: This axis assesses the severity or consequences of a risk event if it were to happen. Consequences can include financial loss, reputational damage, or regulatory sanctions. Like likelihood, impact is also measured on a scale from low to high.

3.6.3 Placing Risks on the Matrix

To use the matrix, each identified risk is evaluated and placed on the grid based on its likelihood and impact. This process involves:

1. **Assessing the Likelihood**: Determine how probable it is for the risk to occur. For instance, consider factors like past incidents, industry trends, and specific vulnerabilities of the institution.
2. **Evaluating the Impact**: Estimate the potential consequences of the risk. This could involve analyzing financial implications, potential damage to the institution's reputation, and the severity of possible regulatory penalties.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

3.6.4 Interpreting the Matrix

Once risks are plotted on the matrix, they can be categorized into different levels of priority:

- **Low Risk**: Risks that are unlikely to occur and would have minimal impact. These require basic monitoring.
- **Medium Risk**: Risks with a moderate likelihood and/or impact. These may necessitate specific mitigation strategies.
- **High Risk**: Risks that are likely to occur and would have significant consequences. These are prioritized for immediate action.

3.6.5 Application in AML/TF

In AML/TF efforts, the risk matrix enables financial institutions to systematically identify, assess, and prioritize risks related to money laundering and terrorist financing. It guides the development of tailored strategies to address high-priority risks, ensuring compliance and safeguarding the institution's integrity.

In our discussions, we've provided an example of a simple 3x3 risk matrix to illustrate how financial institutions can identify, assess, and prioritize risks, particularly in the context of Anti-Money Laundering (AML) and Terrorist Financing (TF). Using this matrix, we can derive 5 distinct risk ratings, which help in categorizing and managing risks more effectively. These ratings are essential for implementing a robust risk management strategy, ensuring that resources are allocated efficiently to mitigate the most significant risks. By understanding and applying these risk ratings within the framework of the risk matrix, institutions can enhance their AML/TF compliance programs, safeguarding against potential threats and ensuring regulatory compliance.

Figure 3.1: Risk Matrix

Probability/Impact	Low	Medium	High
High	High Risk	Very High Risk	Extreme Risk
Medium	Medium Risk	High Risk	Very High Risk
Low	Low Risk	Medium Risk	High Risk

3.6.6 Understanding the Matrix in AML/TF Context

- **Low Risk**: These risks have minimal potential impact and likelihood in the context of AML/TF. For a long-term insurance provider, this might include selling policies to individuals in low-risk employment or residing in low-risk jurisdictions with strong AML regulations.
- **Medium Risk**: Risks with moderate likelihood or impact, such as selling insurance products to companies in industries with higher cash flow but still within jurisdictions known for effective AML/TF controls.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

- **High Risk**: These are significant risks with a high likelihood or impact, such as transactions involving clients based in high-risk countries or sectors prone to money laundering, e.g., clients investing large sums in insurance products that could be used to launder money.
- **Very High Risk**: Represents a very high likelihood or impact, such as doing business with entities or individuals directly linked to high-risk jurisdictions without adequate AML/TF controls, or those previously implicated in financial crimes.
- **Extreme Risk**: The highest risk level, where the likelihood and impact are both considered severe. This could involve facilitating insurance policies for politically exposed persons (PEPs) from jurisdictions with high levels of corruption and weak AML/TF measures, without conducting proper due diligence.

3.6.7 Practical Example: Sarah Creates a Risk Matrix

In the heart of a bustling financial institution, nestled within the gleaming towers of the city's financial district, Sarah, a seasoned compliance officer, sat at her desk surrounded by piles of documents, each one a testament to the complex world of anti-money laundering (AML) and terrorist financing (TF) risk assessment. Her task was daunting yet crucial: to sift through the myriad of potential risk events identified by the institution and assign a risk rating to each, using the institution's 3x3 AML/TF Risk Matrix. This matrix, a beacon in the murky waters of compliance, would guide her in evaluating the likelihood and impact of each risk event, ensuring that the institution could navigate safely through regulatory requirements and avoid the perilous cliffs of non-compliance.

The matrix before her was divided into three columns: Risk Event, Probability, and Impact, with a fourth column reserved for the final Risk Rating. Each row represented a potential risk event, a scenario that, if not properly managed, could lead the institution into the treacherous storm of legal sanctions or the whirlpool of reputational damage.

1. **PEPs as Customers**: The first risk event involved politically exposed persons (PEPs) as customers. Sarah considered the probability as medium; the institution had robust screening processes, yet no system is without its flaws. The impact, however, was undeniably high. The thought of regulatory sanctions sent a shiver down her spine, not to mention the potential for reputational damage if a PEP were to misuse the institution. **Risk Rating: High**

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

2. **Customers from High-risk Countries**: The next line item spoke of customers hailing from countries with weak AML/TF controls. The probability here was glaringly high, a reflection of the institution's global reach and the inherent challenges in vetting such clients. The impact was equally high, the consequences of regulatory non-compliance dire. **Risk Rating: Very High**

3. **High-Risk Products**: Sarah then turned her attention to products with features attractive for laundering activities, such as cash surrender options. Here, the probability was medium, tempered by the institution's product design and monitoring. Yet, the potential misuse of these products for illicit purposes couldn't be ignored, warranting a high impact rating. **Risk Rating: High**

4. **Cash Payments for Premiums**: Cash payments, with their anonymity, presented a high probability of being used for money laundering. The impact was medium, as controls could somewhat mitigate this risk, but the ease of laundering through cash was undeniable. **Risk Rating: High**

5. **Overpayment and Frequent Changes**: Behaviors like overpayment and frequent policy changes were red flags. While not definitive proof of laundering, the probability was medium, with the high impact stemming from the potential for significant financial and reputational harm. **Risk Rating: High**

6. **Use of Third-party Intermediaries**: Reliance on third parties for customer management introduced variability in control effectiveness. With medium ratings for both probability and impact, it underscored the critical nature of due diligence. **Risk Rating: Medium**

7. **Non-face-to-face Business Relationships**: The digital age brought convenience but also risk, with non-face-to-face transactions making customer verification a daunting task. Both probability and impact were high, reflecting the anonymity and reach of digital channels. **Risk Rating: Very High**

With the risk matrix updated, Sarah could see the landscape of AML/TF risks laid out before her. This matrix was not just a tool; it was a map, guiding the institution through the complex terrain of regulatory compliance. By prioritizing resources and implementing targeted mitigation strategies, Sarah could steer the institution away from the risks that loomed largest, ensuring a course true and compliant.

Figure 3.2: 3X3 AML/TF Risk Matrix

Risk Event	Probability	Impact	Risk Rating
PEPS as Customers	Medium	High	High
Customers from High-risk Countries	High	High	Very High
High-Risk Products	Medium	High	High
Cash Payment on Premiums	High	Medium	High
Overpayment and Frequent Changes	Medium	High	High
Use of Third-party intermediaries	Medium	Medium	Medium
Non-face-to-face Business Relationships	High	High	Very High

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

3.7 Create a Risk Register

Creating a Risk Register is a foundational step in the risk management process for Anti-Money Laundering (AML) and Terrorist Financing (TF) within financial institutions. This critical document serves as a comprehensive repository for all identified risks, facilitating systematic tracking and management efforts. The creation of the Risk Register involves several key steps, each aimed at ensuring a thorough understanding and documentation of potential AML/TF risks.

3.7.1 Steps to Create an AML/TF Risk Register

1. Structure the Risk Register

First, define the structure of your Risk Register. Typically, it includes several columns such as Risk Event, Probability, Impact, Risk Rating, Mitigation Strategy, and Assigned Responsibility. At this stage, focus on the first four columns, as they are crucial for identifying and evaluating risks.

2. Compile Identified Risks

Gather all identified AML/TF risks. This compilation should be based on a comprehensive risk identification process that considers various aspects of the organization's operations, including customer base, products and services, geographic locations, and delivery channels.

3. Determine Probability and Impact

For each identified risk, assess the probability of occurrence and the potential impact on the organization. Probability assessments can range from Low, Medium, to High, reflecting the likelihood of the risk event happening. Similarly, impact assessments evaluate the severity of consequences should the risk materialize, also categorized as Low, Medium, or High.

4. Calculate Risk Rating

The Risk Rating is derived by combining the probability and impact assessments. This can be done through a risk matrix, where the intersection of probability and impact levels provides a rating for each risk, such as Low, Medium, High, or Very High. This rating helps prioritize risks based on their overall significance to the organization.

5. Review and Validate

Once the initial Risk Register is compiled, review and validate the information with relevant stakeholders. This includes risk management teams, compliance officers, and department heads. Their insights can ensure that the Risk Register accurately reflects the organization's risk landscape and that all significant risks are captured.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

3.7.2 Practical Considerations

When creating and maintaining an AML/TF Risk Register, it is essential to keep in mind several practical considerations to ensure its effectiveness and relevance over time. These considerations include:

- **Dynamic Document:** The Risk Register is not static. It should be updated regularly to reflect new risks, changes in existing risk assessments, and the effectiveness of mitigation strategies.
- **Comprehensive Coverage:** Ensure that the Risk Register covers all areas of the organization's operations. It should be as exhaustive as possible to avoid overlooking critical risks.
- **Accessibility:** Make the Risk Register accessible to relevant stakeholders while ensuring that sensitive information is adequately protected. Stakeholders should be able to review and contribute to the Risk Register as necessary.

3.7.3 Practical Example: Sarah Creates a Risk Register

Sarah, a dedicated FICA compliance officer at "Fintegrity Financial Services," is tasked with creating an Anti-Money Laundering (AML) and Terrorist Financing (TF) Risk Register. Fintegrity is a growing financial institution that offers a range of services, including loans, savings accounts, and investment products. Recognizing the importance of a robust AML/TF program, Sarah sets out to develop a Risk Register that will help Fintegrity identify, assess, and prioritize its AML/TF risks.

Steps Sarah Follows to Create the Risk Register

1. Structuring the Risk Register

Sarah begins by defining the structure of the Risk Register. She decides to include the following columns for the initial phase:

- **Risk Event:** The description of the AML/TF risk.
- **Probability:** The likelihood of the risk occurring.
- **Impact:** The potential severity of the risk's consequences.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

- **Risk Rating:** An overall assessment combining probability and impact.

Sarah plans to expand the Risk Register later to include mitigation strategies and assigned responsibilities.

2. Identifying Risks

Sarah conducts a series of workshops with various department heads to identify potential AML/TF risks. She also reviews recent audit reports, regulatory findings, and industry risk assessments to ensure she captures a comprehensive list of risks.

3. Assessing Probability and Impact

For each identified risk, Sarah evaluates the probability and impact based on Fintegrity's past experiences, industry data, and regulatory guidance. She uses a scale of Low, Medium, and High to rate both probability and impact.

4. Calculating Risk Rating

Using a simple risk matrix, Sarah calculates the Risk Rating for each risk event. This matrix helps her visually determine which risks require immediate attention and which may be monitored with standard controls.

5. Reviewing with Stakeholders

Sarah presents the draft Risk Register to key stakeholders, including the risk management committee and senior management, for review. This session provides an opportunity for feedback and ensures that all relevant risks are included and accurately assessed.

Table 3.1L AML/TF Risk Register Example

Risk Event	Probability	Impact	Risk Rating	Mitigation Strategy	Assigned Responsibility
PEPS as Customers	Medium	High	High		
Customers from High-risk Countries	High	High	Very High		
High-Risk Products	Medium	High	High		
Cash Payment on Premiums	High	Medium	High		
Overpayment and Frequent Changes	Medium	High	High		
Use of Third-party intermediaries	Medium	Medium	Medium		
Non-face-to-face Business Relationships	High	High	Very High		

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

3.8 Select Appropriate Mitigation Strategy and Assign Responsibility

In the battle against Anti-Money Laundering (AML) and Terrorist Financing (TF), financial institutions adopt a series of dynamic and robust strategies tailored to the complexities of these risks. These strategies are not just theoretical frameworks but practical necessities that are applied based on the specific risk events identified. Let's explore these strategies from a practical viewpoint, emphasizing when and why they are most applicable, illustrated with examples.

The Foundational Strategies are listed here:

- **Customer Due Diligence (CDD):** At the heart of AML/TF mitigation lies Customer Due Diligence. This fundamental strategy involves verifying customer identities, understanding their business activities, and assessing associated risks. Enhanced Due Diligence (EDD) becomes critical when dealing with high-risk customers, such as Politically Exposed Persons (PEPs) or individuals from countries with weak AML controls. For instance, a bank might implement EDD for a new account opened by a foreign government official, scrutinizing the source of funds and monitoring account activities to mitigate potential risks.

- **Transaction Monitoring:** Monitoring transactions continuously allows institutions to spot patterns indicative of money laundering or terrorist financing. Practical application includes setting up automated systems that flag transactions exceeding certain thresholds or those to high-risk jurisdictions, necessitating further investigation. For example, repeated large transactions just below reporting thresholds, a tactic known as "smurfing," would trigger alerts in such systems for further review.

- **Sanctions Screening:** Sanctions screening is a non-negotiable practice involving the comparison of customer names against global sanctions lists. This strategy is crucial for preventing transactions with entities or individuals subject to sanctions. A practical application would be the real-time screening of transaction recipients against updated lists, ensuring compliance and preventing legal repercussions.

- **Risk-Based Approach:** Adopting a risk-based approach means tailoring the intensity of AML/TF controls based on the risk level of customers, products, or regions. This ensures optimal resource allocation. For instance, a bank may apply more stringent controls and monitoring to high-risk products such as anonymous prepaid cards than to low-risk savings accounts.

The advanced strategies are listed here:

- **Use of Technology:** Leveraging technology, including AI and ML, enhances the detection and prevention of AML/TF activities. Practical uses include deploying AI systems for pattern recognition in transaction data, identifying suspicious activities that human analysts might miss. For example, an AI system could detect a complex pattern of transactions that funnel small amounts of money to a common recipient, a potential sign of terrorist financing.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

- **Third-party Management:** For institutions relying on third parties for customer acquisition, due diligence, and continuous monitoring are imperative. This involves vetting third-party partners and regularly auditing their compliance with AML/TF standards. A practical step could be conducting annual audits of third-party vendors to ensure they adhere to contractual AML obligations.
- **Employee Training and Awareness:** Training programs for employees enhance their ability to recognize and respond to AML/TF risks. Practically, this means regular training sessions and updates on AML/TF regulations and methodologies for identifying suspicious activities, ensuring that staff can effectively support the institution's compliance efforts.
- **International Cooperation:** Given the global nature of AML/TF risks, international cooperation is vital for sharing intelligence and best practices. This can take the form of participating in global forums and partnerships to share information on emerging risks and trends, enhancing the collective ability to combat AML/TF activities.

3.8.1 Practical Example: Sarah Selects Mitigating Strategies

In the fast-paced environment of a leading financial institution, Sarah, an experienced compliance officer, found herself at the nexus of regulatory compliance and operational security. Her office, a high-rise amidst the city's financial hub, was a microcosm of the broader battle against money laundering and terrorist financing (AML/TF) risks. With the institution's AML/TF Risk Matrix as her guide, Sarah embarked on a critical mission: to assign risk ratings to various potential risk events and select appropriate mitigation strategies to safeguard the institution.

1. PEPs as Customers

- **Situation:** Sarah faced the challenge of politically exposed persons (PEPs) as customers. Recognizing the medium probability of risk due to existing screening processes, yet acknowledging the high impact of potential regulatory sanctions and reputational damage, she determined a high-risk rating was warranted.
- **Mitigation Strategy:** To combat this, Sarah decided to implement Enhanced Due Diligence (EDD) for PEPs, a strategy involving deeper investigative processes into these customers' backgrounds, sources of wealth, and transaction patterns. This approach aimed to identify and mitigate any potential misuse of the institution's services by PEPs, thereby reducing the risk of regulatory and reputational fallout.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

2. Customers from High-risk Countries

- **Situation:** The next challenge involved customers from countries with weak AML/TF controls. The high probability and impact of risks associated with these clients necessitated a very high-risk rating.
- **Mitigation Strategy:** Sarah opted for stringent Customer Due Diligence (CDD) combined with enhanced ongoing monitoring. This strategy was designed to thoroughly vet the backgrounds and activities of customers from high-risk jurisdictions, ensuring that the institution was not inadvertently facilitating illicit activities.

3. High-Risk Products

- **Situation:** Sarah then assessed products with features attractive for laundering activities, like cash surrender options. With a medium probability and high impact, these products received a high-risk rating.
- **Mitigation Strategy:** Product risk assessment and redesign became her chosen strategy. By evaluating products for vulnerabilities and modifying features to deter misuse, Sarah aimed to strike a balance between commercial viability and security.

4. Cash Payments for Premiums

- **Situation:** The anonymity of cash payments presented a significant AML/TF risk, with a high probability of misuse and a medium impact.
- **Mitigation Strategy:** Limiting cash transactions and enhancing verification for large cash payments was Sarah's strategy of choice. This approach aimed to minimize the institution's exposure to risks associated with cash payments, reducing the likelihood of money laundering.

5. Overpayment and Frequent Changes

- **Situation:** Sarah identified overpayment and frequent policy changes as potential red flags, assigning a high-risk rating due to the medium probability and high impact.
- **Mitigation Strategy:** She implemented transaction monitoring and behavioral analysis to detect and investigate these red flags. By closely monitoring for unusual patterns, Sarah aimed to preemptively address any attempts at laundering through the institution.

6. Use of Third-party Intermediaries

- **Situation:** The use of third-party intermediaries introduced variability in control effectiveness, meriting a medium risk rating.
- **Mitigation Strategy**: Sarah decided on due diligence and continuous monitoring of third parties as the mitigation strategy. Ensuring that third-party partners adhered to the institution's AML/TF standards was crucial for mitigating risks introduced through these channels.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

7. Non-face-to-face Business Relationships

- **Situation:** The digital transformation brought convenience but also heightened risk, with non-face-to-face transactions posing significant AML/TF challenges. The high probability and impact warranted a very high-risk rating.
- **Mitigation Strategy:** Advanced digital identity verification technologies were Sarah's solution. Leveraging biometric verification and other cutting-edge technologies, she aimed to secure the institution's digital channels against potential misuse.

By thoughtfully selecting and implementing these mitigation strategies, Sarah not only ensured compliance with regulatory standards but also fortified the institution against the multifaceted threats of money laundering and terrorist financing. Her work epitomized the critical role of compliance officers in navigating the complex and ever-evolving landscape of financial crime prevention.

Table 3.2 Adjusted Risk Register

Risk Event	Probability	Impact	Risk Rating	Mitigation Strategy	Assigned Responsibility
PEPS as Customers	Medium	High	High	Implement Enhanced Due Diligence (EDD)	
Customers from High-risk Countries	High	High	Very High	Apply Stringent Customer Due Diligence Enhanced Monitoring	
High-Risk Products	Medium	High	High	Product Risk Assessment Redesign	
Cash Payment on Premiums	High	Medium	High	Limit Cash Transactions Enhance Verification	
Overpayment and Frequent Changes	Medium	High	High	Transaction Monitoring Behavioral Analysis	
Use of Third-party intermediaries	Medium	Medium	Medium	Due Diligence Continuous Monitoring of Third Parties	
Non-face-to-face Business Relationships	High	High	Very High	Advanced Digital Identity Verification	

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

3.9 Assign Responsibility

In the complex ecosystem of financial institutions, the effective delegation of Anti-Money Laundering (AML) and Terrorist Financing (TF) mitigation strategies to specific functions or departments is crucial for operational efficiency and regulatory compliance. This chapter discusses the factors to consider when assigning responsibility for mitigation strategies and elaborates on which functions or departments are best suited for particular strategies.

3.9.1 8.1 Understanding Functions and Departments

Before diving into the delegation process, it's important to differentiate between functions and departments within a financial institution:

- **Function:** Refers to a group or a team dedicated to a specific set of tasks or responsibilities, such as compliance, risk management, or customer due diligence.
- **Department:** A larger organizational unit that may encompass multiple functions. For example, the Risk Management Department might include functions such as operational risk, credit risk, and AML/TF risk.

3.9.2 Factors to Consider in Delegation

Several critical factors influence the decision-making process when assigning AML/TF mitigation responsibilities:

- **Expertise and Knowledge:** Assign tasks to departments with the specific expertise needed to effectively implement the mitigation strategy. For instance, Enhanced Due Diligence (EDD) requires a deep understanding of customer profiling, making the Compliance Department a natural fit.
- **Capacity and Resources:** Consider the current workload and resource availability of the department. Overburdening a department without the capacity to take on additional responsibilities can lead to inefficiencies and increased risk.
- **Regulatory Requirements:** Certain regulations may dictate specific responsibilities, requiring departments with the appropriate regulatory knowledge and authority to take charge of certain mitigation strategies.
- **Strategic Importance:** Evaluate the strategic impact of the mitigation strategy on the institution's overall risk posture and allocate responsibilities to departments that align with strategic priorities.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

3.9.3 Delegating Mitigation Strategies: Who Takes What?

1. Compliance Department

- **Mitigation Strategy:** Implementing Enhanced Due Diligence (EDD), Sanctions Screening
- **Rationale:** With their expertise in regulatory requirements and customer verification processes, the Compliance Department is well-equipped to handle EDD and ensure adherence to global sanctions.

2. Risk Management Department

- **Mitigation Strategy:** Product Risk Assessment and Redesign, Transaction Monitoring and Behavioral Analysis
- **Rationale:** This department's expertise in assessing and mitigating risks makes it ideal for overseeing product assessments and monitoring transaction patterns for signs of AML/TF activities.

3. Finance and Operations Team

- **Mitigation Strategy:** Limit Cash Transactions and Enhance Verification
- **Rationale:** Given their role in managing financial transactions and operational controls, this team is suited to implement strategies that reduce the institution's exposure to cash-based money laundering risks.

4. IT and Digital Security Department

- **Mitigation Strategy:** Advanced Digital Identity Verification
- **Rationale:** With their technical expertise, this department can deploy sophisticated identity verification technologies, crucial for mitigating risks in non-face-to-face business relationships.

5. Third-party Management Team

- **Mitigation Strategy:** Due Diligence and Continuous Monitoring of Third Parties
- **Rationale:** This team's focus on managing external partnerships positions it well to conduct thorough due diligence and ensure third-party compliance with AML/TF standards.

6. Human Resources (HR) Department

- **Mitigation Strategy:** Employee Training and Awareness Programs
- **Rationale:** HR's access to all staff members and expertise in training programs make it the ideal department to spearhead education on AML/TF risks and compliance procedures.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

3.9.4 Conclusion

Effective delegation of AML/TF mitigation strategies requires a strategic approach that considers the unique capabilities and resources of each department. By aligning strategies with departments that possess the relevant expertise and capacity, financial institutions can enhance their AML/TF frameworks, ensuring both compliance and operational efficiency.

3.9.5 Practical Example: Sarah Assigns Responsibility

Sarah, tasked with the crucial role of overseeing the allocation of AML/TF mitigation strategies within her financial institution, meticulously reviews the identified risk events. Her goal is to ensure that each mitigation strategy is placed with the department best suited to manage and execute it effectively. Below is a detailed account of her thought process for each risk, her choice of department for the mitigation strategy, and her rationale behind these decisions. Following this analysis is the adjusted risk register reflecting her choices.

Sarah's Decision Process and Rationale

1. PEPs as Customers

- **Choice of Department:** Compliance Department
- **Rationale:** Sarah recognizes the Compliance Department's expertise in regulatory matters and its proficiency in conducting Enhanced Due Diligence (EDD), making it the ideal choice for managing risks associated with PEPs.

2. Customers from High-risk Countries

- **Choice of Department:** AML Compliance Team
- **Rationale:** Given the AML Compliance Team's specialized knowledge in handling the intricacies of international AML standards and their experience with high-risk jurisdictions, Sarah believes they are perfectly positioned to implement stringent CDD and enhanced monitoring.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

3. High-Risk Products

- **Choice of Department:** Product Development Team
- **Rationale:** Understanding the need for a balance between innovation and risk management, Sarah assigns this task to the Product Development Team. Their insight into product features allows them to assess and redesign products to mitigate AML/TF risks effectively.

4. Cash Payment on Premiums

- **Choice of Department:** Finance and Operations Team
- **Rationale:** The operational nature of managing cash transactions leads Sarah to allocate this responsibility to the Finance and Operations Team. Their familiarity with transactional processes ensures they can limit cash transactions and enhance verification efficiently.

5. Overpayment and Frequent Changes

- **Choice of Department:** Risk Management Department
- **Rationale:** Sarah opts for the Risk Management Department due to their analytical capabilities in identifying and interpreting risk patterns, which are crucial for monitoring transactions and behavioral analysis.

6. Use of Third-party Intermediaries

- **Choice of Department:** Vendor Management Office
- **Rationale:** The Vendor Management Office's direct involvement with third-party intermediaries makes them the logical choice. Their established relationships and contractual oversight enable effective due diligence and continuous monitoring.

7. Non-face-to-face Business Relationships

- **Choice of Department:** IT and Digital Security Department
- **Rationale:** With the increasing importance of digital security, Sarah decides that the IT and Digital Security Department is best equipped to handle advanced digital identity verification, thanks to their technical expertise and access to state-of-the-art technologies.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

Table 3.3 Final Risk Register

Risk Event	Probability	Impact	Risk Rating	Mitigation Strategy	Assigned Responsibility
PEPS as Customers	Medium	High	High	Implement Enhanced Due Diligence (EDD)	Compliance Department
Customers from High-risk Countries	High	High	Very High	Apply Stringent Customer Due Diligence Enhanced Monitoring	AML Compliance Team
High-Risk Products	Medium	High	High	Product Risk Assessment Redesign	Product Development Team
Cash Payment on Premiums	High	Medium	High	Limit Cash Transactions Enhance Verification	Finance and Operations Team
Overpayment and Frequent Changes	Medium	High	High	Transaction Monitoring Behavioral Analysis	Risk Management Department
Use of Third-party intermediaries	Medium	Medium	Medium	Due Diligence Continuous Monitoring of Third Parties	Vendor Management Office
Non-face-to-face Business Relationships	High	High	Very High	Advanced Digital Identity Verification	IT and Digital Security Department

3.10 Maintaining Risk Register

Effective monitoring and regular review of the Anti-Money Laundering/Terrorist Financing (AML/TF) Risk Register are essential to ensure that a financial institution's risk management strategies remain relevant and effective. As the risk landscape evolves with new threats, products, and regulatory changes, so too must the strategies to manage these risks. This section outlines practical steps and methodologies for the ongoing monitoring and review of the AML/TF Risk Register, ensuring it remains a dynamic tool in the fight against money laundering and terrorist financing.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

1. Establishing a Review Schedule

- Determine the frequency of reviews based on the risk profile of the institution, with a minimum annual review recommended.
- High-risk areas may require more frequent reviews, possibly quarterly.
- Set specific dates for reviews to ensure they are not overlooked.

2. Pre-Review Preparation

- Collect and analyze relevant data since the last review, including internal audit findings, compliance reports, and incident reports.
- Update information on regulatory changes and industry trends that may impact the risk profile.

3. Involving Key Stakeholders

- Form a review committee including members from compliance, business units, risk management, and senior management to ensure diverse perspectives.
- Engage external experts or consultants when necessary, especially for complex areas or significant changes in the risk environment.

4. Continuous Feedback Loop

- Establish mechanisms for ongoing feedback from employees at all levels, encouraging reporting of potential risks or observations that could impact the risk register.

5. Leveraging Technology for Efficiency

- Use software tools for tracking changes, managing documentation, and facilitating the review process.
- Implement analytics and risk assessment tools to identify trends and anomalies that may indicate emerging risks.

6. Regulatory Alignment

- Regularly update the risk register to reflect changes in AML/TF laws and guidelines, both locally and internationally.
- Document how each regulatory change impacts the institution's risk profile and required actions.

7. Documenting Rationale for Changes

- For every adjustment to the risk register, record the reasoning behind the change, the data or incidents that prompted the change, and the expected impact on risk management strategies.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

8. Reinforcing Training and Awareness

- Update training programs to reflect changes in the risk register, ensuring staff understand new risks and control measures.
- Use the review process as an opportunity to reinforce the importance of AML/TF compliance and the role of the risk register.

9. Incorporating Lessons Learned

- Analyze any AML/TF incidents or near-misses to identify root causes and adjust the risk register accordingly.
- Use these insights to improve preventive and detective controls, and to inform future risk assessments.

3.10.1 Practical Example: Sarah Maintains the Risk Register

Sarah, the diligent FICA compliance officer at Fintegrity Financial Services, understands the importance of keeping the AML/TF Risk Register up-to-date in a rapidly changing risk landscape. She follows a structured approach to ensure the register remains a dynamic and effective tool for managing financial crime risks.

1. Establishing a Review Schedule

Sarah sets a bi-annual review schedule for the entire Risk Register while marking high-risk areas such as cross-border transactions and digital payment platforms for quarterly reviews. She syncs these dates with the company's internal calendar, ensuring they are adhered to by all stakeholders.

2. Pre-Review Preparation

Ahead of each review, Sarah compiles data from various sources within Fintegrity. She gathers internal audit reports, compliance findings, and analyses recent incident logs for any patterns or anomalies. Additionally, she updates her knowledge on the latest regulatory changes and industry trends that could influence Fintegrity's risk profile.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

3. Involving Key Stakeholders

Sarah forms a review committee that includes representatives from compliance, various business units, risk management, and the executive team. She occasionally invites external AML/TF experts to provide fresh perspectives, especially when new types of financial products or services are introduced.

4. Continuous Feedback Loop

She implements a continuous feedback mechanism where employees at all levels can report observations or potential risks anonymously. This input is crucial for identifying emerging threats that might not be captured through formal channels.

5. Leveraging Technology for Efficiency

Sarah uses advanced software tools designed for risk management to track changes in the Risk Register efficiently. She utilizes analytics and risk assessment tools to sift through transaction data, identifying patterns that could indicate new risks.

6. Regulatory Alignment

She ensures that the Risk Register reflects the latest AML/TF laws and guidelines. Each regulatory update is analyzed for its impact on Fintegrity's operations, with necessary adjustments documented in the Risk Register.

7. Documenting Rationale for Changes

For every modification to the Risk Register, Sarah meticulously documents the rationale, supporting data, and anticipated impact on risk management. This documentation is crucial for audits and provides valuable insights for future reviews.

8. Reinforcing Training and Awareness

Post-review, Sarah updates Fintegrity's training programs to include information on new risks and mitigation strategies. She uses these sessions to emphasize the importance of everyone's role in AML/TF compliance and familiarizes them with updates in the Risk Register.

9. Incorporating Lessons Learned

Following any AML/TF incidents or near-misses, Sarah conducts thorough analyses to identify the root causes. She adjusts the Risk Register based on these findings, using the insights gained to enhance Fintegrity's preventive and detective controls.

Through Sarah's meticulous and proactive approach, Fintegrity's AML/TF Risk Register is not just a compliance requirement but a cornerstone of the institution's risk management strategy, evolving continuously to meet the challenges of the financial industry.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

3.11 Practicalities of Implementing a Risk-Based Approach

When implementing a risk-based compliance framework, several critical factors need to be considered to ensure its effectiveness and alignment with organizational goals and regulatory requirements. Here's a comprehensive list of factors that organizations must evaluate:

3.11.1 Risk Assessment

- **Identify and Categorize Risks:** Understand the various types of risks (e.g., operational, financial, legal, reputational) that the organization faces.
- **Risk Analysis:** Assess the likelihood and impact of each risk, considering both internal and external factors.

3.11.2 Regulatory Requirements

- **Compliance with Laws and Regulations**: Ensure the framework aligns with all applicable laws, including international regulations if the organization operates globally.
- **Regulatory Updates:** Stay updated on changes to relevant laws and regulations to adjust the framework accordingly.

3.11.3 Organizational Structure and Culture

- **Roles and Responsibilities:** Define clear roles and responsibilities for compliance within the organization.
- **Culture of Compliance:** Promote a culture that values compliance and ethical conduct at all levels of the organization.

3.11.4 Policies and Procedures

- **Development of Policies:** Create comprehensive policies that outline expected behaviors and compliance procedures.
- **Procedure Manuals:** Develop detailed procedure manuals for critical operations, ensuring they incorporate risk management practices.

3.11.5 Technology and Systems

- **Technology Solutions:** Evaluate and implement technology solutions that support compliance efforts, such as compliance management software.
- **Data Protection:** Ensure systems are in place to protect sensitive data in accordance with privacy laws.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

3.11.6 Training and Education

- **Compliance Training Programs:** Develop and deliver training programs that educate employees on compliance policies, procedures, and risk awareness.
- **Ongoing Education:** Provide regular updates and training sessions to keep staff informed about changes to compliance requirements.

3.11.7 Monitoring and Reporting

- **Continuous Monitoring:** Implement systems for continuous monitoring of compliance risks and the effectiveness of the compliance program.
- **Reporting Mechanisms:** Establish clear reporting mechanisms for compliance issues, including anonymous reporting channels.

3.11.8 Internal and External Communication

- **Stakeholder Communication:** Communicate effectively with all stakeholders about the organization's commitment to compliance and risk management.
- **Regulatory Communication:** Maintain open lines of communication with regulators and other external parties regarding compliance efforts.

3.11.9 Review and Improvement

- **Regular Reviews:** Conduct regular reviews of the compliance framework to assess its effectiveness and identify areas for improvement.
- **Feedback Loop:** Create a feedback loop that allows for the continuous improvement of compliance practices based on insights gathered from monitoring and review activities.

3.11.10 Third-Party Management

- **Vendor and Partner Compliance:** Assess and manage the compliance and risk posture of third-party vendors and partners.
- **Due Diligence:** Perform due diligence on third parties to ensure they adhere to compliance standards that affect the organization.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

3.11.11 Resource Allocation

- **Financial Resources:** Allocate adequate financial resources to support compliance activities, including technology investments and training programs.
- **Human Resources:** Ensure there are sufficient personnel dedicated to compliance roles, with the necessary expertise to manage and mitigate risks.

3.11.12 Emergency Preparedness and Response

- **Incident Response Plan:** Develop and maintain an incident response plan to address compliance breaches or failures promptly.
- **Crisis Management:** Prepare for crisis situations with plans that include compliance considerations to minimize impact.

3.12 Integration of the Risk-based Approach into the RMCP and Policies

A risk-based approach (RBA) is fundamental to an effective Risk Management and Compliance Program (RMCP). It ensures that resources are allocated efficiently, focusing on the most significant risks to organizational objectives. This lesson outlines practical steps for integrating RBA into RMCP and weaving it into the fabric of organizational policies and procedures.

3.12.1 Understanding the Risk-Based Approach

The RBA is a methodological approach to managing and mitigating risks, prioritizing them based on their impact and likelihood. It involves identifying, assessing, monitoring, and controlling risks, with a focus on the most critical ones.

The Benefits of implementing a RBA are as follows:

- Efficient Resource Allocation: Ensures resources are focused on high-impact areas.
- Improved Decision-Making: Facilitates informed choices by highlighting key risk areas.
- Enhanced Compliance: Helps meet regulatory requirements by proactively managing risks.

3.12.2 Embedding RBA into Organizational Policies and Procedures

1. Policy Development and Review

- **Integration:** Ensure that all policies reflect the RBA by incorporating risk management principles.
- **Review Cycle:** Establish a regular review cycle for policies to adjust to the changing risk environment.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

2. Training and Awareness

- **Staff Training:** Equip employees with the knowledge to understand and implement RBA in their daily activities.
- **Culture of Risk Awareness:** Foster a culture where risk management is everyone's responsibility.

3. Communication and Reporting

- **Transparent Communication:** Maintain open channels for reporting risks and discussing risk management activities.
- **Regular Reporting:** Develop a reporting schedule that allows for timely decision-making and adjustments.

3.13 .Internal Controls and Auditing Processes

The RBA under FICA requires institutions to assess the likelihood and impact of financial crime risks, tailoring their compliance programs based on their risk exposure. This approach ensures that resources are allocated efficiently, focusing on higher-risk areas.

3.13.1 Establishing Internal Controls

1. Designing Mitigating Mechanisms

Internal controls are procedures and mechanisms put in place to mitigate risks identified through the RBA. Key controls include:

- Customer Due Diligence: Verifying the identity of clients and understanding the nature of their activities.
- Transaction Monitoring: Implementing systems to monitor customer transactions for suspicious activities.
- Record-Keeping: Maintaining comprehensive records of customer identities, transactions, and due diligence processes.
- Reporting: Establishing protocols for reporting suspicious transactions to relevant authorities.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

2. Best Practices for Effective Mitigating Mechanisms

- **Tailor Controls to Risk:** Customize control measures based on the risk profile of customers, products, and services.
- **Employee Training:** Conduct regular training for employees on FICA obligations and the identification of suspicious activities.
- **Technology Utilization**: Leverage technology to enhance the efficiency and effectiveness of compliance measures.

3.13.2 Auditing Processes for FICA Compliance

1. Planning the Audit

- **Scope and Objectives:** Define the scope and objectives of the audit, focusing on areas of highest risk as identified by the RBA.
- **Audit Team:** Assemble an audit team with the necessary expertise in FICA compliance and risk management.

2. Conducting the Audit

- **Review of Internal Controls:** Assess the design and operational effectiveness of internal controls in managing identified risks.
- **Compliance Testing:** Perform tests to evaluate compliance with CDD, record-keeping, reporting, and other FICA requirements.
- **Risk Management Assessment:** Examine the institution's process for identifying, assessing, and managing financial crime risks.

3. Reporting and Recommendations

- **Audit Report:** Compile findings, including deficiencies in internal controls and non-compliance with FICA.
- **Actionable Recommendations:** Provide recommendations for improving compliance and strengthening internal controls.

4. Follow-Up and Continuous Improvement

- **Implementation of Recommendations:** Monitor the institution's efforts to implement audit recommendations.
- **Continuous Monitoring:** Advocate for ongoing monitoring and periodic audits to adapt to changes in risk exposure and regulatory requirements.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

3.14 Collaboration with Regulatory Bodies for FICA Compliance

Compliance with the Financial Intelligence Centre Act (FICA) is a critical aspect of operating within the financial sector. For Financial Service Providers (FSPs), this involves not only adhering to stringent regulations aimed at preventing financial crimes but also ensuring transparent and ongoing communication with regulatory bodies like the Financial Sector Conduct Authority (FSCA). This chapter explores the importance of collaboration between organizations and regulatory bodies to achieve and maintain FICA compliance.

3.14.1 The Importance of Collaboration

Collaborating with regulatory bodies is pivotal for organizations aiming to navigate the complexities of FICA compliance effectively. This partnership plays a critical role in:

- Ensuring Compliance: Regular interaction with regulatory bodies helps organizations understand their compliance obligations under FICA. This includes clarity on customer due diligence, record-keeping, reporting suspicious transactions, and implementing a risk-based approach.
- Staying Informed on Legislative Changes: Regulatory frameworks are dynamic, with frequent updates to address emerging financial crimes. Collaboration with regulatory bodies ensures that organizations are informed about legislative changes, enabling them to adapt their compliance programs promptly.
- Mitigating Risks: Close collaboration helps identify potential compliance risks early, allowing organizations to implement corrective measures before issues escalate. This proactive approach can prevent financial penalties and reputational damage.

3.14.2 Strategies for Effective Collaboration

To foster effective collaboration with regulatory bodies and ensure FICA compliance, organizations can employ the following strategies:

- Regular Communication: Establish and maintain open lines of communication with regulatory bodies. This can involve attending workshops, seminars, and meetings hosted by the FSCA or FIC.
- Compliance Reporting: For FSPs, annual FICA compliance reporting to the FSCA is mandatory. Ensure these reports are comprehensive, accurate, and submitted on time. Use these reports as an opportunity to demonstrate your organization's commitment to compliance.
- Seeking Guidance: Do not hesitate to seek guidance from regulatory bodies on complex compliance issues. This can prevent potential non-compliance and demonstrates a proactive approach to regulatory adherence.
- Participating in Regulatory Programs: Engage in programs and initiatives led by regulatory bodies designed to enhance the industry's understanding and implementation of FICA. This can include pilot programs, feedback sessions, and joint task forces.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

3.14.3 Building a Compliance Culture

Building a robust compliance culture within an organization is crucial for ensuring adherence to the Financial Intelligence Centre Act (FICA) and fostering positive relations with regulatory bodies. Key elements of creating and maintaining this culture include:

- Leadership Engagement: Ensure that top management shows a strong commitment to compliance, setting a tone at the top that emphasizes the importance of ethical conduct and adherence to regulatory requirements.
- Training and Awareness: Regularly train employees on FICA obligations and the importance of collaboration with regulatory bodies. Awareness programs can help embed a culture of compliance throughout the organization.
- Continuous Improvement: Treat compliance as an ongoing process. Continuously evaluate and improve your compliance measures based on feedback from regulatory bodies and changes in the regulatory landscape.

3.15 Evaluating the Effectiveness

In the context of the Financial Intelligence Centre Act (FICA) compliance, the adoption of a Risk-Based Approach (RBA) and a comprehensive Risk Management and Compliance Program (RMCP) is essential for organizations operating within the financial sector. These frameworks are designed not only to comply with legal requirements but also to safeguard the organization against financial crimes effectively. This chapter outlines practical steps and metrics for evaluating the effectiveness of RBA and RMCP in the context of FICA implementation, ensuring that organizations can assess their compliance strategies' impact on financial stability and regulatory adherence.

3.15.1 Key Performance Indicators for Evaluation

1. **Reduction of Financial Crime Incidents**

- **Metric:** Track and compare the frequency and severity of financial crime incidents before and after RBA implementation.
- **Data Source:** Incident reports, investigation outcomes.

2. **Improvement in Customer Due Diligence (CDD) Processes**

- **Metric:** Measure the accuracy and completeness of CDD processes, including the identification and verification of customer information.
- **Data Source:** CDD audits, customer verification records.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,

3. Enhanced Risk Management Strategies

- **Metric:** Evaluate the effectiveness of risk identification, assessment, mitigation, and monitoring processes.
- **Data Source:** Risk assessment reports, risk mitigation action plans.

4. Increased Regulatory Compliance

- **Metric:** Assess compliance with FICA requirements, including reporting obligations and record-keeping standards.
- **Data Source:** Compliance audit findings, regulatory inspection reports.

3.15.2 Evaluation Techniques

- **Internal Audits:** Conduct regular internal audits to assess the effectiveness of the RBA and RMCP. Focus on compliance with policies, the efficiency of risk management practices, and adherence to regulatory requirements.
- **External Audits and Assessments:** Engage independent external auditors to provide an unbiased evaluation of the organization's compliance framework. This can help identify gaps not evident to internal teams.
- **Compliance Testing:** Perform targeted compliance testing of specific areas, such as CDD procedures and suspicious activity reporting, to assess adherence to FICA regulations and internal policies.
- **Stakeholder Feedback:** Gather feedback from employees, customers, and regulators on the organization's risk management and compliance efforts. This feedback can offer valuable insights into areas for improvement.

3.15.3 Regular Reviews and Continuous Improvement

- **Conducting Periodic Reviews:** Establish a schedule for regular reviews of the RBA and RMCP to ensure they remain effective and responsive to changes in the risk environment and regulatory landscape.
- **Implementing Improvement Plans:** Based on evaluation findings, develop and implement action plans to address deficiencies, enhance controls, and improve compliance measures.
- **Staying Ahead of Evolving Threats:** Incorporate intelligence on emerging financial crime threats into the risk assessment process to ensure proactive management of new risks.

©2024, Compliance and Learning Center (Pty) Ltd. All rights reserved,