

Final

Breaking down the FIC Act: A Quick Guide for Accountable Institutions

As is generally the case with new legislation, most businesses will only take it seriously once an inspector comes knocking. This should not be the case. Although the FIC Act (FICA) was created to prevent financial crime, following the guidelines set out in the Act will also help businesses protect their reputation and enhance client onboarding, while reducing their risk and ultimately attracting a more desirable clientele. With this in mind, compliance should be viewed by Accountable Institutions as an opportunity and be approached proactively, says Sameer Kumandan, Managing Director of [SearchWorks](#), an innovative data platform that allows businesses to conduct accurate, in-depth KYC checks online.

Why is the FIC Act so important?

The FIC Act holds immense significance for South Africa's financial system and national security on multiple fronts. Primarily, it acts as a powerful weapon in the fight against financial crime, addressing issues like money laundering, terrorist financing, and corruption. By disrupting the financial networks of criminals and terrorist organisations, the Act contributes to the stability and integrity of South Africa's financial system, safeguarding its reputation to attract foreign investment.

From a consumer perspective, the legislation acts as a shield by preventing financial scams and identity theft, to foster greater trust in the financial sector. In terms of national security, the Act plays a critical role in reducing the risk of terrorist attacks and impeding organised crime. Additionally, by aligning with international standards, the FIC Act promotes global cooperation, strengthening the collective effort against illegal financing. In essence, this legislation is indispensable in ensuring a resilient, secure, and inclusive financial environment for South Africa.

What are the key elements of the FIC Act?

The FIC Act is aimed at preventing financial crime in South Africa by addressing Money Laundering (ML), Terrorist Financing (TF), and the financing of the Proliferation of Weapons of Mass Destruction (WMD). At its core, the legislation establishes the Financial Intelligence Centre (FIC), an independent agency responsible for receiving, analysing, and disseminating financial intelligence reports. The FIC is authorised to collaborate with law enforcement agencies to guide accountable institutions and support investigations and prosecutions that are related to financial crime.

To this end, accountable institutions are required to adhere to Anti-Money Laundering and Counter-Terrorism Financing (AML/CFT) obligations, which include customer identity verification, transaction monitoring, risk mitigation measures, and staff training for compliance. The Act also puts in place clear reporting thresholds and triggers for suspicious transactions and financial indicators.

What does compliance with the FIC Act entail?

Adhering to compliance expectations under the FIC Act involves implementing an internal Anti-Money Laundering and Counter-Terrorism Financing (AML/CFT) program, which includes the establishment of robust policies, procedures, and controls for managing Money Laundering (ML) and Terrorist Financing (TF) risks.

A critical aspect of compliance in this regard requires accountable institutions to conduct a thorough risk assessment to identify and evaluate ML/TF risks specific to the business and its clientele. Customer due diligence (CDD) practices will determine the verification of customer identities based on assessed risk levels, while the Know Your Customer (KYC) process will require a more in-depth understanding of customer backgrounds, business activities, and the sources of funds.

To play their part, accountable institutions are responsible for the timely reporting of suspicious transactions and activities to the Financial Intelligence Centre (FIC) through Suspicious Activity Reports (SARs). Such institutions will also need to implement meticulous record-keeping of transactions and customer information for a specified period (a minimum of five years) while conducting employee training on AML/CFT procedures and the recognition of suspicious activities.

Who/what are accountable institutions?

While the full list of "accountable institutions" can be found in Section 1 of the Act, generally speaking, an institution is considered accountable if it is an entity susceptible to being used for ML/TF. This includes banks, credit providers, securities firms, and insurance companies; as well as dealers in cash, precious metals, and gemstones, along with attorneys, accountants, and auditors. The list also includes casinos and other gambling businesses, money or value transfer services, and real estate agents and property developers.

How can SearchWorks help?

SearchWorks can assist accountable institutions ensure they carry out their due diligence in terms of accurate KYC (know your customer) and KYB (know your business) checks,

accurately and without hassle. Our data aggregation platform provides comprehensive information on individuals, businesses, trusts, and properties in South Africa, offering various search types suitable for purposes like KYC, AML/CFT, and due diligence.

With a commitment to full compliance with the FIC Act, SearchWorks encourages organisations to leverage this requirement to create additional business value. By reducing fraud, safeguarding reputation and capital, and streamlining reporting and compliance duties, organisations can effectively navigate and benefit from regulatory pressures.