

FAIS Newsletter



Financial Services Board

04/12/2017

Volume 25

From the FIC Desk:

The journey to FICA compliance



Introduction

The theme of this Newsletter is compliance with the Financial Intelligence Centre Act (FIC Act). In this issue, we provide a high level overview of the key changes in the FIC Act and the possible implications to authorised financial services providers (FSPs) designated as accountable institutions. We take FSPs through a journey towards implementing the new provisions of the FIC Act and meeting their obligations.

In the forthcoming issues of the Newsletter, we will unpack some of the new provisions of the FIC Act and provide detailed information that may be of interest to you.

Inside this issue:



From the FIC Desk:	1
The journey to FICA compliance	1
Introduction	1
Why the FIC Act was amended	2
Commencement of the FIC Act	2
Status of Exemptions and ML/TF Control Regulations	2
Overview of the new provisions	3
The road ahead	7
Implication for FSPs	7
Important FICA documents	8
Regulatory expectations	8
Supervision and enforcement	9
Contact Details	11

Disclaimer

This newsletter does not constitute a Guidance Note as envisaged in the FIC Act. The FIC is the only statutory body that is empowered in terms of section 4(c) of the FIC Act to issue guidance on matters of compliance with the FIC Act. The Newsletter should not be construed as a substitution of the FIC Act or ML/TF Control Regulations. It does not take away the obligations that are imposed on accountable institutions. The Newsletter has been published for information purposes only.

Why the FIC Act was amended

As part of an on-going effort to strengthen the Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) measures in South Africa, National Treasury and the Financial Intelligence Centre (FIC) have amended the FIC Act. The amendments are designed to bring South Africa's AML/CFT legislative framework in line with the Standards set out by the Financial Action Task Force (FATF) and international best practices. The amendments are also intended to augment South Africa's position in combating money laundering and terrorist financing, and strengthen its capacity to prevent financial crimes and to discipline such crimes.

Commencement of the FIC Act

A phased approach has been adopted towards the commencement of the FIC Act. Different parts of the Act commenced on different dates as follows:

- The first provisions of the FIC Act commenced on 13 June 2017. These provisions did not require changes to ML/TF Control Regulations, Exemptions or internal processes and systems of accountable institutions to enable compliance with the FIC Act. The provisions dealt mainly with dissolving the CMLAC, information sharing, consultation arrangements with stakeholders, concerns relating to inspection powers and warrants, and improvement of the appeal process.
- The bulk of the provisions came into effect on 2 October 2017. These provisions required changes to ML/TF Control Regulations and withdrawal of Exemptions, as well

as training of staff and major changes to processes and systems used by accountable institutions.

- The commencement date of the remaining provisions relating to the freezing of assets in terms of the United Nations Security Council Resolutions on targeted financial sanctions will still be determined.

Status of Exemptions and ML/TF Control Regulations

The FIC Act is now a principles-based piece of legislation. It sets out broad obligations for accountable institutions, but leaves the methods of meeting those obligations to be decided by the accountable institutions. This implies that accountable institutions should determine the most appropriate means to implement the provisions of the FIC Act.

Previously, accountable institutions relied on Exemptions and other information that was prescribed in the ML/TF Control Regulations. The Exemptions have been withdrawn and the ML/TF Control Regulations have been amended to make way for a risk-based approach.

A risk-based approach provides accountable institutions with the flexibility to use a range of mechanisms towards implementation of the FIC Act and encourages accountable institutions to explore innovative ways of offering financial services to their broader client-base. It must be noted that accountable institutions may continue to be guided by the contents of some of the withdrawn Exemptions in the implementation of their compliance approaches.

Overview of the new provisions

The new provisions introduce new concepts and approaches to the application of the FIC Act. Below is a summary of the new provisions that came into effect on 2 October 2017:

(i) Risk-based approach – The implementation of the new requirements in the FIC Act requires a sound assessment and understanding of the potential ML/TF risks facing the business.

As of 2 October 2017, accountable institutions are expected to adopt a risk-based approach. The risk-based approach requires the accountable institution to identify and assess the ML/TF risks it can reasonably expect to face in the course of its business. These risks may arise from various factors, such as clients, products and services, delivery channels and geographic locations. The accountable institution should then apply its knowledge and understanding of the ML/TF risks to develop control measures to prevent, mitigate or manage those risks.

A risk-based approach assumes that accountable institutions are best placed to know their products and services, clients, operating structure and business environment. It also assumes that accountable institutions are best placed to assess the risk that their business may be used for ML/TF purposes.

(ii) Risk Management & Compliance Programmes (section 42) - As of 2 October 2017, every accountable institution is required to develop, document, maintain and implement a Risk Management and Compliance Programme (RMCP), which replaces the internal rules.

A risk assessment is the first step the accountable institution should undertake

before developing a RMCP. In developing its RMCP, the accountable institution should take into account the nature, size and complexity of the business.

Please note the following regarding the RMCP:

- It should set out policies and procedures used to identify and assess ML/TF risks emanating from products & services, clients, delivery channels and geographic locations.
- It should also set out the internal policies, procedures and controls necessary to monitor; mitigate; and manage the ML/TF risks arising from products & services, clients, delivery channels and geographic locations.
- It must be approved by senior management.
- Accountable institutions should review and update it on a regular basis to keep up with the rapidly changing business environment in which accountable institutions operate.

(iii) Anonymous clients (section 20A) - accountable institutions are prohibited from establishing a business relationship or entering into a single transaction with an anonymous client or a client with an apparent false or fictitious name.

(iv) Identification of clients (section 21) - when the accountable institution engages with a prospective client to establish a business relationship or conclude a single transaction, it is required to establish and verify:

- the identity of the client;
- or identity of the person acting on behalf of the client;
- or identity of the client acting on behalf of the person.

The identification and verification of clients is one of the most important requirements. It affects other obligations imposed by the FIC Act. For example, reporting obligations cannot be carried out effectively if the accountable institution has insufficient knowledge regarding the identity of the client.

(v) Customer due diligence (section 21A) - refers to information and documents obtained about a client which could assist the accountable institution to mitigate ML/TF risks that may be identified from doing business with a client.

Customer due diligence starts with the requirement imposed on accountable institution to establish and verify the identity of the client. The accountable institution should then obtain information about the business relationship to enable it to determine whether future transactions that will be performed in the course of that business relationship are consistent with the accountable institution's knowledge of that prospective client. The information that should be obtained relates to:

- The nature of the business relationship;
- The intended purpose of the business relationship; and
- The source of funds to be used in the course of a business relationship.

The extent of the customer due diligence measures applied should be commensurate with the level of risk posed by the client type, products and services, business relationship, single transactions, distribution channels and geographical locations. Where ML/TF risks are assessed as low, simplified measures may be applied. Where there are higher ML/TF risks, enhanced measures should be

applied to mitigate those risks. Accountable institutions are not required to carry out the full scope of customer due diligence measures in respect of clients conducting occasional or once-off single transactions below R5 000.

(vi) Additional due diligence (section 21B)

– This section applies to legal persons (i.e. close corporations, companies or any form of corporate arrangement or association), trusts and partnerships. If a client is a legal person or natural person acting on behalf of a trust or partnership, the accountable institution is required to:

- Determine the nature of the business relationship;
- Determine the ownership and control structures of the client; and
- Identify beneficial owners of the legal person.

The following criteria may be adopted to identify beneficial ownership of a legal person:

- Identify natural persons who ultimately own the legal person
 - *If there is doubt that these natural persons are not the beneficial owners or if there are no such natural persons, then*
- Identify those natural persons who ultimately control the legal person or have ultimate effective control of the legal person
 - *If there is doubt that these natural persons are not the beneficial owners or if there are no such natural persons, then*
- Identify natural those persons who have executive authority over the legal person, or are in equivalent or similar positions

(vii) Ongoing due diligence (section 21C)

– accountable institutions are required to conduct ongoing due diligence in respect of a business relationship, including:

- monitoring transactions (such as source of funds, background and purpose of all complex and unusual transactions) undertaken throughout the course of a business relationship.
- keeping documents, data or information obtained for the purposes of establishing and verifying the identities of clients up to date and relevant.

(ix) Doubts about veracity of previously obtained information (Section 21D)

- Accountable institution is required to repeat the steps set out in sections 21, 21A and 21B of the FIC Act if there are doubts about the adequacy or veracity of previously obtained information which the accountable institution is required to verify.

(x) Inability to conduct customer due diligence (Section 21E)

- if the accountable institution is unable to establish or verify a client's identity, or conduct due diligence on the client, the accountable institution should not establish a business relationship or conclude a single transaction with such a client; or continue to conclude a transaction in the course of a business relationship with a client. The accountable institution is also required to submit a suspicious transaction report to the FIC.

(xi) Section 21F and 21G introduce the concepts of foreign prominent public officials and domestic prominent influential persons respectively as well as their known family members and close associates under **section 21H**. In the past,

these individuals were referred to as "politically exposed persons" (PEPs). These individuals occupy positions that may be abused for the purpose of committing ML/TF offences.

The FIC Act provides for a number of mechanisms to deal with these individuals. Accountable institutions are required to make a determination, in accordance with their RMCP, whether these individuals present a heightened risk to the accountable institution's business. The accountable institution will then have to take reasonable measures to determine the source of their wealth or origin of their funds used in respect of a particular transaction. The accountable institution should also obtain senior management approval to enter into a business relationship or conclude single transactions with them. Finally, the accountable institution is required to conduct enhanced ongoing monitoring of the business relationship with a view to identifying unusual or suspicious transactions.

(xii) Record keeping (sections 22 and 22A)

– accountable institutions are required to keep records of transactions with clients, information relating to a business relationship, and customer due diligence information obtained from a client or prospective client under section 21 to 21H of the FIC Act.

(xiii) Section 26A and 26B have not come into effect yet. The sections deal with the prohibitions on dealings with persons and entities identified by the Security Council of the United Nations. Accountable institutions will need to have procedures and controls in place to give effect to the requirement to freeze assets in accordance with the United Nations Security Council Resolutions. Accountable institutions will have to ensure that

effective mechanisms are in place to communicate designations by the United Nations Security Council under various Resolutions. They will also have to establish screening procedures to determine whether a client is affected by a designation.

(xiv) Reporting obligations (section 28, 28A and 29) - In accordance with the FIC Act and ML/TF Control Regulations, accountable institutions and reporting institutions are required to submit reports to the FIC on suspicious and unusual transactions, cash transactions over R24 999.99 and transactions related to property owned or controlled by or on behalf of a terrorist. Accountable institutions are referred to Guidance Notes 4A, 5B and 6 for assistance on how to complete these regulatory reports.

The FIC analyses the reports and generates financial intelligence information which is handed over to relevant authorities for further action or investigation if necessary.

(xv) AML/CFT compliance governance (section 42A) – (NB: In the case of a legal person, senior management is the board of directors. In the case of an accountable institution without a board of directors, senior management are those persons who are responsible for the management of the accountable institution).

The board of directors of an accountable institution which is a legal person or senior management of an accountable institution without a board of directors, are responsible for ensuring compliance by both the accountable institution and its employees with the provisions of both the FIC Act and the RMCP.

In the case of an accountable institution which is not a legal person, the person or persons exercising the highest level of

authority in the business should take responsibility for compliance by both the accountable institution and its employees.

(xvi) Responsibility for compliance function (section 42A) – The accountable institution, which is a legal person, is required to establish a compliance function to assist the board of directors or senior management.

The accountable institution which is a legal person (i.e. close corporation, company or any form of corporate arrangement or association), is required to assign a person with sufficient competence and seniority to ensure effectiveness of the compliance function.

An accountable institution which is not a legal person i.e. a trust and partnership (except for a sole proprietor) should appoint a person or persons with sufficient competence to assist the person or persons exercising the highest level of authority in the business to ensure compliance with the FIC Act by the accountable institution and its employees.

In the case of sole proprietors, the buck stops with them. The FIC Act does not place an obligation on them to appoint person to assist in ensuring compliance. Sole proprietors exercise the highest level of authority in the business and should take responsibility for ensuring compliance with the FIC Act.

The FIC defines a Compliance Officer as a person who is tasked, for purposes of the registration and reporting process, to ensure that the details of the accountable institution are correctly submitted and maintained on the FIC's website. The Compliance Officer should be distinguished from the Money Laundering Reporting Officer (MLRO). According to the FIC, the MLRO is envisaged to be a person, other than the Compliance

Officer, with the responsibility and authority to submit regulatory reports to the FIC on behalf of the accountable institution or reporting institution. Therefore, not all accountable institutions or reporting institutions will have a Compliance officer or MLRO. The MLRO will have his or her own login credentials on goAML.

(xvii) Training (section 43) – The accountable institution is required to provide its employees with ongoing training to enable them to comply with the FIC Act and the RMCP; and to discharge the specific responsibilities assigned to them. Please note that accountable institutions with no employees are also subject to ongoing training.

(xviii) Registration with the FIC (section 43B) - accountable institutions and reporting institutions are required to register with the FIC. All previously registered accountable institutions and reporting institutions should have been migrated to the new goAML system by now. All institutions need to ensure that their registration information with the FIC is kept up to date at all times. The FIC will maintain a register of all registered institutions.

The road ahead



We would now turn to how we will ensure that FSPs are ready for the above-mentioned changes.

Implication for FSPs

The commencement of the FIC Act marked the beginning of a journey to compliance. Many FSPs could find this journey difficult if they do not invest early the amount of time and effort and the resources needed to implement the new provisions.

The phased approach to the commencement of the FIC Act as well as the transitional period allowed by the FSB may both be deemed to have afforded FSPs enough time to familiarise themselves with their obligations prior to the cut-off date for enforcing compliance.

As of 02 October 2017, FSPs should ensure that their current systems, processes, procedures and controls are rigorous enough to meet the new requirements introduced by the FIC Act. However, this may be a challenge for smaller FSPs. As stated in our previous newsletter, the ability and capacity to comply with the new provisions may not be the same for both large and smaller entities. The ability to implement the new requirements depends on the state of readiness robustness of the systems, processes, procedures and controls.

Survey - we indicated in our previous newsletter that the FSB would circulate a survey to authorised FSPs to assess the state of readiness to implement the new provisions of the FIC Act. The responses to the survey will determine the cut-off date by which the FSB will start enforcing compliance with the new provisions.

Please note that the FSB will no longer circulate the survey because the FIC has already emailed it to all accountable institutions registered with it. To re-circulate the survey would have been burdensome for FSPs, resulting in unnecessary duplication of information.

We would like to thank those FSPs who responded to the survey. The FIC has shared your responses with us. The results of the survey show that the majority of the FSPs indicated that they would be ready by 1 December 2018 to implement the new provisions of the FIC Act as they needed more time to amend existing processes and/or systems. The FSB will therefore delay enforcing compliance with the new provisions of the FIC Act to 30 November 2018. As of 1 December 2018, FSPs are expected to be fully compliant as administrative sanctions will be issued for breaches of the new requirements.

FSPs are encouraged to implement the new provisions of the FIC Act at the earliest opportunity and not to wait until the cut-off date. Some FSPs have the capacity and the necessary resources to meet the expectations much faster than others. Those that are well equipped may already be well down the road on a journey to implement the new provisions. Those further down the road would have noticed that it takes a combination of factors such as people, processes, and systems to implement the requirements.

Important FICA documents

The FIC provides valuable information on a regular basis to help accountable institutions understand their obligations under the FIC Act. The FIC has published documents on its website (www.fic.gov.za) in the lead up to commencement of the FIC Act. The documents that have been published so far include:

- The FIC Amendment Act;
- ML/TF Control Regulations;
- Guidance Note 4A – to assist accountable institutions, reporting institutions and any other person to whom the FIC Act applies in

meeting their reporting obligations in terms of section 29 of the Act;

- Guidance Note 5B – to assist accountable institutions and reporting institutions in meeting their cash threshold reporting obligations in terms of section 28 of the FIC Act;
- Guidance Note 6 – provides guidance on terrorist financing and terrorist property reporting obligations in terms of section 28A of the FIC Act; and
- Guidance Note 7 – to assist accountable institutions on the implementation of the various provisions of the FIC Act.

FSPs are encouraged to familiarise themselves with these documents because they contain valuable information that they would need to implement the requirements of the FIC Act.

Regulatory expectations

It is fundamentally important that FSPs adapt to and demonstrate compliance with the new obligations in as timely a manner as possible, so the objectives of the FIC Act can be achieved.

We expect the FSP and its staff to be clear about their obligations to comply with the FIC Act, and for senior management and directors to make sure that they know what the FSP should be doing to comply.

FSPs should develop and implement systems and processes or optimise existing ones to ensure compliance with the new requirements. FSPs should adopt a robust approach to managing and monitoring compliance with the FIC Act.

A range of guidance material is already available on the FIC's website to help you get started. The FIC have also issued

Guidance Note 7 and ML/TF Control Regulations to assist accountable institutions in meeting their obligations. We encourage FSPs to utilise these resources.

Please note that while a concerted effort will be made to provide support and assistance to FSPs on a regular basis, there won't be an easy 'tick box' path towards achieving compliance. An approach, driven solely by a desire to meet regulatory expectations rather than truly address the ML/TF risks, may not necessarily enhance overall systems, controls and processes. FSPs should make a concerted effort to know and familiarise themselves with the law, understand their obligations, know their business and ML/TF risks facing them, and then make decisions about how to manage and mitigate those risks.

Supervision and enforcement



We will continue to use a variety of supervisory tools, from desk based reviews of compliance reports to on-site inspections, to monitor and supervise compliance with the FIC Act. Support is available to help you understand and do what is required as follows:

Education and assistance - We will continue engaging FSPs to make sure they understand their obligations. With effect from March 2018, the FAIS Supervision department will be traveling to certain parts of the country to conduct interactive workshops with small and medium sized

FSPs without compliance officers to present important information about the new provisions of the FIC Act and to discuss the obligations imposed on them. The details of the venues, dates and times will be published on the FSB's website in due course.

Newsletter - We will continue to keep you updated on regulatory developments through various communication channels, including the FAIS Newsletter. In the forthcoming issues of the Newsletter, we will publish detailed articles on some of the new provisions of the FIC Act that came into effect on 2 October 2017. We hope to include practical examples where possible to enhance your understanding of the requirements that may appear complex.

Compliance reports – we have developed a separate compliance report for FSPs focusing on compliance with the FIC Act only. Further details regarding the consultation process and any assistance that may be deemed necessary prior to the completion of the first standalone FICA compliance report will be published in due course.

Onsite inspections – We will proactively conduct onsite inspections to a range of FSPs to assess compliance with the FIC Act. During the inspections, FSPs will be expected to demonstrate compliance towards the new requirements. The focus of the inspections is to determine whether FSPs have appropriate systems, controls, processes and procedures in place to meet their regulatory obligations and mitigate against identified or perceived ML/TF risks.

Sanctions – Please note that responsibility for compliance with the FIC Act rests with the FSP and its board of directors or senior management. Where

our inspections identify non-compliance, we will use a range of measures available to us, to elicit a timely, effective and proportionate response from the affected FSPs. Sanctioning non-compliance with the new requirements may be delayed until 1 December 2018, however, the affected FSPs will be directed to apply and demonstrate active remediation on the non-compliant areas. Administrative sanctions will be imposed on non-

compliance with the current provisions of the FIC Act that are not amended, such as registration and reporting obligations.

Contact Details

Contact Centre:	0800 11 04 43 0800 20 20 87
Switchboard:	+27 12 428 8000
Facsimile:	+27 12 346 6941
Media Queries:	+27 12 422 2823
Email Us:	info@fsb.co.za
Anonymous Fraud & Ethics Tip Offs Hot-Line:	0800 31 36 26
Anonymous Fraud & Ethics email:	fsb@whistleblowing.co.za
For technical queries:	web.master@fsb.co.za

Addresses

Physical	Riverwalk Office Park, Block B 41 Matroosberg Road (Corner Garsfontein and Matroosberg Roads) Ashlea Gardens, Extension 6 Menlo Park Pretoria, South Africa, 0081
Postal	P.O. Box 35655 Menlo Park 0102

E-mail inboxes:

Purpose	Inbox
General FAIS related enquiries.	Faisinfo@fsb.co.za
Submission of profile change requests specifically relating to FSPs.	Faispfc@fsb.co.za
Submission of the excel rep import spread sheet. This e-mail address should only be used where the person submitting the excel spreadsheet is registered to submit on behalf of the FSP. Where the person is not registered to submit an excel spreadsheet on behalf of the FSP then the request should be sent to the faispfc@fsb.co.za inbox.	Reps@fsb.co.za
Submission of any requests to lapse licenses and	Fais.Lapse@fsb.co.za

Purpose	Inbox
enquiries relating to lapse requests that have been submitted.	
Requests for duplicate copies of FAIS licenses and annexures. Please ensure that proof of payment accompanies the request for a duplicate license copy.	Fais.Licensecopies@fsb.co.za
E-mail submissions of new license applications for FSPs.	Fais.Newlicense@fsb.co.za
E-mail submissions for application for phase 1 approval of compliance officers	Fais.COapprovals@fsb.co.za
Submission of specimen mandates for approval.	Fais.Mandates@fsb.co.za
All queries relating to the regulatory examinations e.g. queries related to duplicate certificates, how to register for exams, authentication etc.	Fais.Exams@fsb.co.za
Queries relating to qualifications e.g. credits, recognition of qualifications.	Fais.Qualifications@fsb.co.za
Queries relating to the Fit and Proper Requirements e.g. new entrants wanting to know what competency requirements they have to meet.	Fitandproper@fsb.co.za
Submission of documents and queries in response to an intention to suspend or suspension letter sent to an FSP.	Fais.Compliance@fsb.co.za
Extension requests for the submission of annual financial statements.	Faisfins2@fsb.co.za
Extension requests for the submission of annual financial statements.	Faisfins3@fsb.co.za
Queries on compliance reports and queries related to the FAIS online reporting system.	Faiscomp1@fsb.co.za
Submission of FAIS related complaints against key individuals, representatives and FSPs.	FaisComplaints@fsb.co.za
Submission of debarment notifications relating to representatives.	Debarment@fsb.co.za
Submission of exemption applications for exemptions specific to a person or FSP.	Fais.Exemptions@fsb.co.za
Submission of excel spread sheets to register for the regulatory examination exemptions that published under Board Notice 102 of 2012.	Fais.Examexemptions@fsb.co.za
Submission of proof that conditions associated with exemptions that were granted have been complied with.	Fais.conditions@fsb.co.za
Submission of DOFA related enquiries and requests for DOFA reports.	Fais.Dofa@fsb.co.za