TC NOTES

PRACTICAL **LEADERSHIP**
AND **GUIDANCE** FROM
TORONTO CENTRE

SUPERVISION OF MONEY LAUNDERING AND TERRORIST FINANCING

MONITORING COMPLIANCE BY FINANCIAL INSTITUTIONS WITH THEIR AML/CFT OBLIGATIONS

UPDATED VERSION

OCTOBER 2020

TORONTOCENTRE
Global Leadership in Financial Supervision

Global Affairs Canada
Affaires mondiales Canada

Sida
SWEDISH INTERNATIONAL DEVELOPMENT COOPERATION AGENCY

SUPERVISION OF MONEY LAUNDERING AND TERRORIST FINANCING

MONITORING COMPLIANCE BY FINANCIAL INSTITUTIONS WITH THEIR AML/CFT OBLIGATIONS

TABLE OF CONTENTS

SUPERVISION OF MONEY LAUNDERING AND TERRORIST FINANCING

MONITORING COMPLIANCE BY FINANCIAL INSTITUTIONS WITH THEIR AML/CFT OBLIGATIONS

Introduction[1]

This Toronto Centre Note provides guidance for the supervision of the implementation by financial institutions (FIs) of their obligations to implement measures to combat money laundering (ML) and terrorist financing (TF). Where applicable, this guidance could also apply to compliance with similar obligations by Designated Non-Financial Business and Professions (DNFBPs).

The standards for combatting ML and TF are established by the Financial Action Task Force (FATF) and apply to a wide range of law enforcement and other agencies. One key element of the FATF Standards is the obligations placed on FIs and DNFBPs. The Standards also set out minimum requirements for supervisors.

This Note focuses on the actions to be taken by supervisors to ensure implementation of these obligations. The Note provides an overview of the obligations placed on FIs and DNFBPs, but for detailed guidance, reference should be made to the FATF Recommendations themselves,[2] particularly Recommendations 9 to 23 and the methodology for assessing compliance.[3] Other relevant standards are issued by other bodies, such as the Basel Committee on Banking Supervision.[4]

In many countries, the supervisor with responsibility for the supervision of compliance by FIs and DNFBPs with prudential and conduct of business requirements is also responsible for monitoring compliance with AML/CFT obligations. However, in some cases, other agencies, such as the Financial Intelligence Unit (FIU), are responsible for monitoring compliance with AML/CFT obligations. This Note is intended to apply to any supervisor with responsibility for AML/CFT obligations. Where the FIU also has supervisory functions, the guidance should be read as if referring to the relations between the different departments of the FIU responsible for supervision and for receiving and analyzing reports respectively.

Objectives of supervision of AML/CFT obligations

The objectives of the supervision of AML/CFT obligations are to:

- develop a full understanding of ML/TF risks faced by FIs and DNFBPs subject to supervision;

[1] This Note was prepared by Richard Pratt. It replaces an earlier version published in February 2016.
[2] FATF (2019a).
[3] FATF (2019c).
[4] Basel Committee (2020).

- set obligations on FIs and DNFBPs that meet the FATF Standards and are tailored to the specific risks of ML and TF in the jurisdiction, taking account of the objective of financial inclusion;
- set and implement obligations in a way that is consistent with other objectives – particularly for financial inclusion;
- ensure that each institution with relevant obligations understands its own ML/TF risks;
- prevent criminals and others who may permit or facilitate ML or TF from owning or controlling FIs and DNFBPs;
- strengthen the governance of FIs and DNFBPs particularly with respect to ML/TF risk management, and raise the awareness of management of their obligations;
- monitor the effectiveness of FIs and DNFBPs in adopting, documenting, implementing, and reviewing policies and procedures to undertake appropriate customer due diligence; and
- ensure that FIs and DNFBPs maintain appropriate records to demonstrate compliance, to facilitate investigations, and to freeze funds related to money laundering and terrorist financing.

Overview of FI and DNFBP obligations

The FIs and DNFBPs on which obligations are imposed are described in the glossary to the FATF Recommendations. The main financial institutions include banks, insurance companies, securities firms, exchanges, and clearing houses. DNFBPs are a broad range of specified professions and bodies, including lawyers, accountants, firms supplying services to companies and trusts, casinos, real estate agents, and dealers in high-value goods.

The FATF Recommendations expect both supervised entities and supervisory authorities to adopt a **risk-based approach**, as defined in Recommendation 1 (R1) of the FATF Recommendations.[5] The obligation on each FI and DNFBP is that they should assess and document the ML and TF risks arising from their business; adopt policies and procedures to mitigate those risks; monitor the effectiveness of those measures; and take enhanced measures when higher risks are identified. The measures taken by each FI and DNFBP must, of course, meet the minimum standards imposed by the supervisor, but should also go further – to mitigate the risks as assessed by each FI and DNFBP.

The **customer due diligence** (CDD) obligations encompass a detailed set of actions (R10 and R22). The FI or DNFBNP must take reasonable measures to establish and verify who the customer is, on whose behalf the customer is acting, what business the customer undertakes, and what ML/TF risks the customer poses. This is the basis on which the FI or DNFBP must detect and report suspicious activity (R20 and R23).

Each FI and DNFBP must develop risk-based systems of **internal controls** that encompass the implementation of policies and procedures and the vetting and training of staff (R18). The controls should include the creation of an internal compliance arrangement and an internal audit function. They should apply the AML/CFT controls to foreign branches and subsidiaries. The standard defines the circumstances and extent to which reliance can be placed on third parties to undertake CDD (R17). The **record keeping** obligation is to keep information for at least five

[5] See FATF (2007).

years so that customer files can be reviewed and transactions reconstructed. Files must be made available to the authorities (R11).

All countries are required to implement **United Nations sanctions on terrorism and nuclear proliferation**. One aspect of the implementation of the sanctions is that FIs and DNFBPs should comply with orders to freeze the assets of persons designated under specified UN sanctions and for preventing other people from making assets or other resources available to such designated persons. FIs and DNFBPs should report the assets they have frozen under these sanctions (R6 and R7).

The risk-based approach to supervision

The FATF Recommendations require the adoption of a **risk-based approach**[6] to all aspects of the design and implementation of a supervisory regime to combat ML and TF. Each country must undertake a national risk assessment (NRA) of the ML and TF risks facing the jurisdiction (R1). There should be widespread participation in the development of the NRA. The supervisor should take a prominent role in identifying ML/TF risks – particularly those that arise within the regulated community.

In addition to contributing to the NRA, the supervisor should undertake a risk assessment of the financial services business and DNFBPs for whose general oversight the supervisor is responsible. The precise structure of such an assessment is for the supervisor to determine, but the assessment should cover the ML and TF risks arising from:

- the **customers** served by the regulated community (for example, retail, professional, high net worth);
- the **markets** targeted and served (for example, domestic or foreign, general or niche, wholesale or retail);
- the range of **products and services** offered (for example, deposit taking and lending, general and life insurance, securities brokerage, fund management, creation of structured products, virtual assets); and
- the **delivery mechanisms** by which the products and services are provided (for example, face to face, by the internet, through mobile phones, directly or through intermediaries or agents).

In addition, the risk assessment should consider the extent to which the risks are exacerbated by weaknesses in the AML/CFT defences. Such weaknesses may arise because of gaps in regulatory requirements, poor compliance by FIs and DNFBPs, ineffective enforcement by the supervisor or other agencies, or other weaknesses such as inadequate coordination between the relevant domestic agencies among themselves or with their foreign counterparts.

The supervisor should also undertake a separate risk assessment of each individual FI or DNFBP within its jurisdiction. This assessment should also consider the risks posed by the customers, markets, products/services, and delivery channels of each supervised institution, together with an assessment of its effectiveness in developing and implementing its AML/CFT

[6] This risk-based approach is similar to the more general risk-based approach to supervision, as described in Toronto Centre (2018).

defences. The assessment of strengths and weaknesses should encompass the adequacy of the institution's own risk assessment, its governance arrangements, the nature of the AML/CFT measures, and the effectiveness of its controls. The effectiveness of an institution's own risk-based approach should be one of the key parameters in the supervisor's own risk scoring of institutions.

The supervisor's risk assessment of individual institutions should preferably be conducted in a way that leads to a separate scoring for each institution. The supervisor should seek to develop a series of parameters, each of which should be given a score. Each parameter should be given a weighting. The objective would be to develop an overall ranking of institutions and a deeper understanding of the nature of the risks posed.

The risk scoring should be updated annually, or whenever there is significant new information, such as after an on-site inspection or following a periodic return submitted by the institution. The supervisor should regularly review the scoring parameters in the light of market developments and other trends and the knowledge gained from regular supervision.

The purpose of the risk assessments is to develop an objective basis for the determination of the supervisor's priorities and resource allocation. This should govern the supervisor's planned actions in respect of the use of its supervisory tools. For example, the overall risk assessment of the business for whose oversight the supervisor is responsible should lead to the supervisor's priorities for regulatory development – what additional rules or regulations are necessary to address the highest risks? What simplified due diligence may be permitted and in what circumstances? What regulatory gaps should be filled first? This assessment should also guide the supervisor's priorities in determining the criteria for assessing applications for authorization or for the approval of senior managers and directors, what guidance to give institutions, what periodic reports to require, and which regulatory breaches should be subject to the most severe sanctions.

The risk scoring of individual institutions should determine periodic reporting requirements tailored for institutions in a specific sector and for individual institutions; the frequency and scope of management meetings with institutions; the nature and frequency of on-site inspections; and the nature and severity of enforcement actions.

Since the purpose of the risk assessment is to determine priorities so as to make most effective use of limited supervisory resources, it follows that the risk assessments must be robust. It should be brutally honest in identifying the matters giving rise to ML/TF risks, even if such an assessment reveals inadequacies in the supervisor's practices hitherto. Only through such honesty can the risk assessment be useful in identifying priority actions for the future.

The use of supervisory tools

The supervisor has a wide range of supervisory tools to be used to implement effective AML/CFT defences. It is sometimes believed that the monitoring of the implementation of AML/CFT obligations should be undertaken primarily though on-site inspections and that the purpose of risk scoring is to determine the order of priority of such inspections. This approach is unlikely to lead to the most effective use of supervisory resources. On-site inspections are important and are an essential tool in the supervisor's armoury. However, inspections, when

undertaken thoroughly, are very resource-intensive and in most cases are not undertaken very frequently. The supervisor needs to make full use of all its supervisory tools as described below.

The overall approach should be to use all available methods to ensure a regular flow of information about implementation of AML/CFT defences from institutions and to ensure that institutions receive regular information from the supervisor, for example about trends and typologies. Inspections should be used on a reasonably regular basis (no less frequently than once every four years) to check that the information provided by the institution is accurate, and on an ad hoc basis where intensive supervision is required in a particular case.

Standard setting: the legal instruments for FATF Standards

The FATF Recommendations require that the basic obligations to conduct CDD (R10), to keep records (R11), and to make reports (R20) should be imposed through primary legislation, enacted by Parliament, or through legally binding case law created by judicial decisions. All other obligations may be imposed through some other enforceable means that are legally binding on those to whom they are directed. The supervisor must be able to apply sanctions where breaches of the requirements are found. Sanctions should be effective, proportionate, and dissuasive.

Customer due diligence
The supervisor must apply its risk-based approach to the setting of the key requirement that FIs and DNFBPs should undertake appropriate, risk-based customer due diligence (CDD).

The core purpose of CDD is to ensure the FI or DNFBP knows who the customer is and the nature of the business that is being done. The identity of the customer must be verified using independent documentation or information. The person on whose behalf the customer is acting and the beneficial owner of the account must also be established. The purpose of the business relationship and the source of funds used to establish the relationship must be known. This information must be known before the business relationship becomes operational – unless it is essential to carry out some activity in advance of completing CDD and the risks of so doing are properly managed.

The extent and depth of the due diligence measures should be determined on the basis of the risks posed by the customer. The FI or DNFBP must then build a profile of expected activity and take measures to monitor the actual activity against this profile. Procedures must be in place to identify transactions and activity that depart from this profile. Reviews of the customer's ML and TF risks should take place periodically (more frequently for higher risk customers) and when an activity or transaction departs from the profile or is otherwise unusual or suspicious. The review should reassess the risk and, where the review gives rise to a suspicion that ML or TF may be involved, the FI or DNFBP must report to the FIU (R20 and R23). There should be no indication to the customer that a report has been made (R21 and R23).

CDD measures for specific kinds of customer and other ML/TF risk, such as politically exposed persons, correspondent banks, money or value transfer services, new technologies, wire transfers, and customers from high-risk countries) are also required by the standards (R12 to R16 and R19).

In each case, the underlying principles are the same. The FI or DNFBP must make an assessment of risk, deploy appropriate risk mitigation measures, and ensure there is an understanding of who the customer or counterpart is.

Beneficial ownership

A central theme running through the FATF Recommendations is that an FI or DNFBP should take reasonable measures to satisfy itself that it knows who the beneficial owner is.[7] The beneficial owner is defined as "the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted." It also includes those persons who exercise ultimate effective control over a legal person or arrangement. The determination of beneficial ownership is important because money launderers may well wish to hide their identity and one way of achieving this is to operate an account through someone else. It is therefore vital that an FI or DNFBP is required to ask each of their customers whether or not they are acting solely on their own behalf or, at least in part, for someone else. This applies whether or not the customer is a natural person, a legal person, or a legal arrangement.

There are many examples of where a beneficial owner may differ from the person opening an account. Some examples include:

- a person acting with a power of attorney
- a lawyer or accountant operating an account for a client
- a person operating a joint account
- the owners of a legal person or arrangement that owns a company opening an account
- the controllers of a substantial proportion (which may be as low as 25%) of a legal person, where that concentration of ownership gives substantial influence or even control
- the trustees, settlor, or beneficiaries of a trust

Virtual assets

One example of new technology, to which the FATF Recommendations refer in R16, is the development of virtual assets.[8] The FATF Recommendations define these as "digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes." Virtual assets do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations.

Examples of virtual assets include assets that are often referred to as virtual currencies, such as bitcoin. For the purpose of FATF guidance, the focus is on assets that are convertible into fiat currencies or interact in some way with the fiat financial system. The risks posed by these assets arise largely because of their unfamiliarity to supervisors and the scope they give for hiding the identity of those who own and trade the assets. In most cases, transactions will be undertaken remotely and not face to face. They will often involve cross border transactions.

Supervisors must participate in a national risk assessment (NRA) of the risks posed by virtual assets and virtual asset service providers. On the basis of the risk assessment, the competent

[7] See FATF (2018).
[8] See FATF (2019b) for detailed guidance on the regulation and supervision of virtual assets.

authorities should determine what virtual assets may be permitted within the jurisdiction and, for those that are permitted, which of those businesses who provide services to people using virtual assets should be subject to regulation and supervision. They should require regulation and supervision of those service providers that facilitate exchange between virtual assets and fiat currencies or the exchange or transfer between different virtual assets. Safekeeping of virtual assets (for example through the provision of wallets) and the provision of financial services to those wishing to buy or sell virtual assets should also prompt a requirement to be regulated. The requirement for regulation is in the country where the assets are created although supervisors may wish to insist on licensing or registration before any service provider based in a foreign country conducts business in their country. All regulated service providers must be subject to the preventive measures set out in the FATF Recommendations. For example, they must make a risk assessment of their products and services, conduct risk-based CDD, monitor activity, keep records, have proper internal controls, and report suspicions.

Digital identity

When considering what forms of identity verification could be acceptable as part of the CDD process, the supervisor will need to consider the growing availability of digital identity technologies.[9] Digital ID refers to the process where a digital ID service provider establishes the identity of a person (using documents, references, and other means) and determines credentials that the person has (such as knowledge of passwords, biometric information, or other means) so that a third party with access to the system can be confident that the person presenting the credentials is the person they claim to be.

There are many benefits to the CDD process from such a system. They can be more reliable than traditional methods, save costs, be easier for the customer, and may promote financial inclusion. However, they carry risks in that cyber-attacks or security breaches may have a very substantial effect. These risks can be mitigated.

Some governmental authorities, for example in the United States and the European Union, have set assurance standards for digital identity systems. These determine the levels of assurance and hence the confidence that supervisors can have in the reliability of the systems and the effectiveness of their measures to mitigate the risks.

Supervisors will need to understand the basic principles of digital identity systems and to satisfy themselves that any such systems they may wish to permit to be used as part of the CDD process have been properly tested and meet the standards set by the jurisdiction (or if there are no country-specific standards, the standards set by the US or EU). Supervisors should make a risk assessment to determine if the system they propose to use is appropriate given the ML and TF risks in their jurisdiction. FIs and DNFBPs who wish to use them should also be required to demonstrate an understanding of the systems and to make a risk assessment of the impact of the use of digital ID systems in the context of their business.

Enhanced and simplified CDD

Each jurisdiction is expected to have in place the basic AML/CFT defences as required by the FATF Recommendations. However, in addition, supervisors should have regard to the NRA and their own assessment of the ML/TF risks of the business undertaken by institutions, to consider whether there should be enhanced measures to take account of specific risks, or areas where there could be simplified measures. For example, in jurisdictions where political corruption is

[9] See FATF (2020) for guidance on digital identity.

perceived to be widespread, the supervisor may consider that it is appropriate to introduce additional measures to require FIs and DNFBPs to undertake enhanced CDD measures for certain categories of domestic politically exposed persons (PEPs), as well as foreign PEPs, even though the FATF Recommendations do not require all enhanced CDD measures for foreign PEPs to be applied to domestic PEPs.

On the other hand, there may be characteristics of the financial sector that allow the supervisor to permit simplified measures to be taken by FIs and DNFBPs. This may be true for certain basic insurance products, for example. There may be scope for simplification where an FI customer is a publicly-owned institution. Simplified measures may well be necessary to promote financial inclusion, which is discussed further below.

This Note does not offer specific guidance as to the enhanced or simplified measures that should be applied as this will vary according to the ML and TF risks of each jurisdiction. However, the essential point is that, under the risk-based approach now required by the FATF Recommendations, supervisors should look beyond the specific requirements of the Recommendations and use the standard-setting power to build stronger defences where ML/TF risks are greater, while allowing simplified measures where the risks are lower. While it is acknowledged that not all supervisors have the power to set binding rules purely at their own discretion, it is usually the case that supervisors are in a position to recommend the provisions that should be included in binding regulations for AML/CFT obligations on institutions.

Financial inclusion[10]

In most countries, there are people who do not have access to the formal financial sector. This may be for many reasons. However, one important reason, especially in developing countries, is that people do not have ready access to the documentation needed to establish and verify identity. This is especially true for women.

The risk-based approach permits supervisors to promote financial inclusion by simplifying due diligence requirements, where there is low risk. While not all those who are financially excluded are necessarily low risk, supervisors can mitigate the risk in other ways. For example, a number of countries allow a single document, such as government ID, a reference letter, or biometric ID to be sufficient – where the customer is provided with only basic financial services. This could be a bank account (or mobile phone account) with a limited number and/or size of transactions. Some countries have adopted a tiered approach with more extensive CDD requirements linked to more sophisticated and extensive financial services offered for higher tiers.

The FATF has indicated that, in certain circumstances, it may be possible to exempt very low-risk customers, using very low-risk products, from CDD altogether, although no mutual evaluation review has yet identified a supervisor who has done this.

The use of digital identity systems can promote financial inclusion where the system has robust and flexible means of establishing the identity of people for whom official documentation is hard to obtain. However, if the preferred digital ID system in a country only uses official documentation, the use of such systems may actually inhibit financial inclusion. So, it is important, where financial inclusion is an objective, that supervisors make sure the system they wish to deploy is appropriate to their circumstances and promotes rather than inhibits financial inclusion.

[10] See also Alliance for Financial Inclusion (2018).

An important factor of promoting financial inclusion is the widespread use of mobile money. This can take many forms, such as the use of smartphone apps to link directly to bank accounts and make transactions. In addition, especially in sub-Saharan Africa, customers with no bank accounts can use mobile phone accounts to transfer money between different account holders. Cash can be placed onto and withdrawn from mobile money accounts, often using agents. In some cases, mobile phones can be used to make payments to merchants. Mobile money is not normally a virtual asset (as defined above), since it is a digital representation of fiat currency. The money tends to be denominated in fiat currency and transfers are linked, directly or indirectly, to real transfers of fiat currency through the banking system.

Mobile money carries risks that have to be taken into account in the decision on how best to encourage financial inclusion through this mechanism. One clear risk is that agents – who may often be very remote from the bank or mobile phone company that is supplying the service – may not be well supervised. They may not be conducting CDD appropriately or may even be using their position as a hub for many mobile users to operate ML or even TF schemes themselves.

The essential point in determining the nature of any simplified or special CDD arrangements to promote financial inclusion is that the supervisor should make a risk assessment of the service and determine how best to mitigate that risk. Any banks or other service providers who are facilitating products and services to promote financial inclusion must themselves also be required to make a risk assessment of the product and service and show how they are mitigating that risk.

Governance requirements

One risk that is frequently realized in practice is that the management of financial institutions and DNFBPs fail to give sufficient attention to the implementation of AML/CFT defences, as routine administrative tasks tend to be delegated to junior officials. It is important for the supervisor to set standards of governance to address this risk.

For example, supervisors may consider imposing (or recommend the imposition of) regulations that include the following:

- give the board the responsibility to make a risk assessment and require the board to review the risk assessment regularly;
- insist that the risk assessment includes or is accompanied by a statement of the board's risk appetite, which defines the risks the board is prepared to accept and those it is not, taking account of ML/TF risks posed by customers, markets, products/services, and delivery channels;
- oblige the board to adopt policies and procedures designed to mitigate the risks and to review regularly the effectiveness of those policies and procedures;
- create an obligation for a reliable management information system to give the board indicators as to the effectiveness of the AML/CFT controls;
- provide for a minimum number of non-executive board members, with perhaps an exemption for single traders or other very small businesses;
- create an obligation to prepare a statement of matters delegated to executives; and

- require the board to consider a report from a compliance officer on the efficacy of AML/CFT defences no less frequently than annually and to ensure that the internal audit program regularly reviews the effectiveness of AML/CFT policies and procedures.

Consultation on standard setting
It is good practice for the supervisor to consult the regulated community about all new or amended regulations. This is clearly important where the supervisor wishes to require enhanced measures, to permit simplified measures on the basis of the risk assessment, or to impose governance requirements that may go beyond those specified in international standards. The consultation should include a written statement of the enhanced or simplified measures or the governance measures and the reasons for them. The use of workshops and industry discussions is helpful, but there is no substitute for a written expression of the supervisor's proposals and reasoning. Following the consultation, the supervisor should make public its response by summarizing the responses received in relation to each enhanced or simplified measure and giving the supervisor's response to the comments – whether accepting them in whole or in part and amending the proposal or rejecting them.

The supervisor should review on a regular basis the continuing necessity of such enhanced measures, or the justification for simplified measures.

Authorization of FIs and DNFBPs

Setting appropriate criteria
The FATF Recommendations require supervisors to take action to prevent criminals from owning or controlling FIs and DNFBPs (R26). In addition, supervisors need to be in a position to reject applications that pose an unacceptable ML or TF risk. It is important that authorization criteria are drawn sufficiently broadly to allow the supervisor to make and defend such a judgement.

The supervisor must have the power to assess owners and controllers of FIs and DNFBPs both at the time of the application for authorization and whenever there is a new owner or controller. It follows that supervisors must ensure that they have the power to seek information from applicants (and their associated persons) about owners and controllers. Applicants, owners, and controllers should be required to be truthful in responding to requests for information. Supervisors must also be able to require FIs and DNFBPs to seek prior approval before any new owner or controller is appointed or acquires control.

The supervisor will need to consider who should be regarded as an owner or controller for the purposes of these requirements. The definitions will depend on the structure and legal form of the institution. The definition must include those with a significant direct or indirect ownership interest and those in a position to influence significantly the business and activities of the institution. The definition should include, for example, the board members, directors responsible for operations and finance (where these are not also board members), as well as the person responsible for monitoring compliance and for assessing potential suspicious transaction reports.

International standards generally define the criteria for granting authorization in terms of fitness and properness. The term fit and proper is normally defined as encompassing competence,

integrity, and financial standing. It is important that supervisors should apply these criteria separately to the applicant itself as a legal organization, to the owners, and to the controllers.

Assessing the criteria

For the applicant for authorization (which will normally be a legal entity), the competence criterion means that the legal entity should have directors and staff who, taken as a whole, have sufficient skills for the business it intends to do and to manage the risks (especially, in this context, the ML/TF risks) to which it is subject. The assessment of this criterion is separate from that of individual directors, since this criterion refers to the balance of skills available to the applicant institution. It is possible for an applicant to have directors, all of whom are individually fit and proper but whom, taken together, may not have the balance of skills necessary to run the business and manage the ML and TF risks.

The integrity criterion means that the applicant should have appropriate governance arrangements and that there should be no history of regulatory non-compliance, and no criminal investigations associated with that entity. There should be financial resources sufficient to support the risks of the business.

For the owners, the criteria should require reasonable business skills (although not specific skills for the business if they are not active in management). They should be required to declare any investigations or findings by law enforcement, regulatory, or professional bodies, or by previous employers, even if such investigations did not lead to any specific sanctions. The supervisor should then use the information to judge whether or not the integrity criterion is met. Their financial circumstances should be sufficiently robust to avoid the risk that they may be vulnerable to pressure from money launderers, terrorist financiers, or others.

For the controllers, the criteria should be the same as for the owners except that the competence criteria will need to be more specific as to the nature of the business and the management of ML and TF risks. For certain posts, the supervisor may wish to specify the minimum competence criteria and this should enable the supervisor to judge the capacity of the controllers to assess and manage the entity's ML and TF risks.

When assessing the applications, the supervisor will need to consult all relevant authorities for information on whether or not the applicant, the owners, or the controllers pose an ML or TF risk. The agencies to be consulted should include the FIU, law enforcement, and other regulatory bodies (both domestic and foreign) where the owners or controllers have worked or in whose jurisdiction the applicant (or affiliated company) has operated.

In addition to assessing the competence, integrity, and financial standing of the applicants, owner, and controllers, the supervisor will also wish to satisfy itself that the applicant has the willingness and capacity to comply with its obligations (including AML/CFT requirements). This will certainly include an assessment of the governance arrangements in line with the standards suggested above. In addition, there should be an assessment of the business strategy and business model to determine whether the revenue received is likely to be sufficient to enable the applicant to conduct CDD and other obligations to the standard required.

Giving reasons for decisions

The supervisor must be in a position to reject (or insist on the rejection of) an applicant (or individual owners or controllers) that does not meet the criteria. It is particularly important to be able to reject applications that pose an unacceptable ML/TF risk. It follows that authorization criteria must be drawn in such a way that the supervisor is able to refer to published criteria when it considers that an applicant poses an unacceptable ML/TF risk.

Where applications are rejected or authorization conditions are imposed, the supervisor will be required to give reasons. Supervisors will have to be mindful of the confidentiality of information they may have received from the FIU and other agencies. They should seek to ensure that reasons for rejection can be given publicly and that there is no risk of being forced to grant authorization solely because the information on which the supervisor relies to defend a rejection cannot be made public.

Raising awareness of AML/CFT obligations

Supervisors have a range of opportunities for raising awareness of AML/CFT obligations.

Public guidance
Public guidance, that is not legally binding, cannot be used to implement the obligations required by the FATF Recommendations. As noted above, the FATF preventive measures must be implemented by law or other enforceable means. Nevertheless, non-binding guidance can be useful in raising the awareness of FIs and DNFBPs of the nature of the mandatory obligations imposed through more formal instruments.

In particular, it is useful for a supervisor to issue guidance, giving examples of the kinds of detailed measures that should be put in place to meet the legally binding requirements. The supervisor may often find it helpful to make clear to FIs and DNFBPs that, although the suggested measures in the guidance are not binding in themselves, the supervisor would expect FIs and DNFBPs to adopt the measures in the guidance unless they can demonstrate that they have adopted other measures that can be shown to be equally effective at meeting the legal obligations.

Two examples may help to illustrate this point:

1. There should be a legally binding obligation on the FI or DNFBP to undertake a risk assessment and keep it up to date. The supervisor could issue non-binding guidance as to the form such an assessment should take and the way in which it should be undertaken by the institution, the trigger factors that might prompt a review, and the minimum frequency of such reviews.

2. There should be a legally binding requirement to apply customer due diligence measures and to perform enhanced due diligence where the ML/TF risks are higher. Guidance could give more detail on the methods that could be used to assess the risks posed by customers and the nature of enhanced due diligence for higher risk customers.

Non-binding guidance of this kind can also be used to give examples of best practice. Where some FIs or DNFBPs find ways of meeting the legal obligations that are more efficient or appropriate in their context than the measures in the guidance, the supervisor may find it helpful

to amend the guidance so as to spread information on more innovative ways of meeting the obligations.

Industry and management meetings

The management of each FI and DNFBP has the prime responsibility for making a risk assessment and managing ML/TF risks accordingly. Regular meetings between the supervisor and management are useful ways of monitoring the extent to which the managers of FIs and DNFBPs are exercising their responsibility and gaining a better understanding of the development of risks in the sector. The supervisor will always meet senior management as part of an on-site inspection, but the supervisor should also make sure that such meetings take place more frequently than the inspection cycle. For FIs and DNFBPs that are significant in the jurisdiction, this should be no less frequently than annually.

The supervisor should determine the agenda for management meetings on the basis of its own risk assessment of ML/TF risks in the domestic business and also the risk scoring of the institution whose management the supervisor is meeting. Subject to that, the supervisor can use such meetings to assess management awareness of their ML/TF responsibilities and to strengthen management's understanding of the risk-based approach. The supervisor can also use such meetings to raise issues that have arisen in the course of other monitoring activity – such as the information provided through periodic reports and the results of on-site inspections.

Meetings with the management of individual FIs and DNFBPs can also help increase the supervisor's knowledge of their governance practices and provide an opportunity for the supervisor to raise awareness of good governance standards relevant to AML/CFT defences. The supervisor can discuss the risk assessment of the FI or DNFBP and test the management's understanding of their assessment, the policies and procedures, and the management information systems designed to provide information on the effectiveness of the AML/CFT defences.

Meetings with groups of FIs and DNFBPs or with industry trade associations can be used to raise awareness of common issues. This can be a useful way of reaching smaller FIs and DNFBPs for whom it may not be realistic to have annual meetings with management.[11] Again, the agenda should be based on the supervisor's risk assessment. Subject to that, the common issues might include the information and guidance issued by the FATF, trends and typologies that have been detected by the FIU, and common compliance weaknesses found by the supervisor. The supervisor may wish to give feedback on the quality of reporting (perhaps by including the FIU at such meetings). The meetings could also be used to spread understanding of good practice.

Meetings with the industry representatives can also be useful in providing feedback to the supervisor about problems in achieving full compliance and alternative solutions for meeting the main AML/CFT obligations set out in law. The supervisor can also use such meetings to review enforcement action and provide guidance on the implications of such action for the compliance procedures of all FIs and DNFBPs.

Public statements

[11] This is similar to the risk-based approach to the supervision of smaller firms more generally, as described in Toronto Centre (2020).

Some of the information that the supervisor may give to industry representatives (as set out above) may also be issued in the form of public statements. For example, there could be public statements on enforcement actions, trends, and typologies. Public statements could be issued to provide specific information, for example on terrorist financing sanctions and on prevalent examples of financial abuse of FIs and DNFBPs.

Monitoring implementation of AML/CFT obligations

Supervisors have a range of tools available to monitor the implementation of AML/CFT defences.

Periodic reporting
Most supervisors place obligations on institutions to make periodic reports on a monthly, quarterly, and/or annual basis. In most cases, these reports concern the financial condition of the institution. However, there are also categories of information that could be obtained from periodic reports that can provide useful information on the state of compliance with AML/CFT obligations.

The precise selection of the information to be required in periodic reports should be determined on the basis of the risk assessment. Some examples of periodic reporting requirements are set out below:

- Risk assessment
- Business plan
- Customer acceptance policy
- Customer acceptance procedure
- Risk scoring methodology
- Customers in different risk categories
- Customers/beneficial owners by business/location
- Complaints
- Number of PEPs
- Internal audit plan & reports
- Compliance officer reports
- STRs received by MLRO and not submitted to FIU
- Office manuals
- Training needs analysis
- Training records
- Staff sanctions
- Results of tests of third-party records
- Analysis of refused business

Information from institutions on their own risk assessment, business plan, and various policies and procedures can be analyzed to determine whether the institution has something in place and to judge its quality. Data on customers in risk categories, the breakdown of customers by location or business, complaints, and the number of politically exposed persons (PEPs) can be helpful in judging the risks of the institution and in determining whether it is implementing the kind of management information system that would enable it to keep track of risks and the effectiveness of policies and procedures in mitigating such risks. Reports issued by the compliance officer and the internal auditor can demonstrate whether such reports are being made and, if so, their quality and effectiveness. It is also possible to use the information in such reports to assess risk and to discuss risks with management at management meetings.

Information on the number of internal reports of suspicious transactions can be compared with the number of reports actually submitted to the FIU. A supervisor might well expect that there should be a considerable number of internal reports that would be made to the compliance

officer (or money laundering reporting officer, if different) that would not be forwarded to the FIU. This would usually be because an institution would wish to ensure that all suspicious transactions were reported internally, and to achieve this the internal bar for reporting could be set at a lower level than the threshold required to make a report to the FIU. An institution that forwards all internal reports to the FIU may not be detecting all relevant suspicions.

Alternatively, an institution that has a large number of internal reports of which few are reported to the FIU may be wrongly holding back reports. While such data cannot be definitive on their own, they should identify industry outliers and may prompt questions for the supervisor to raise at meetings with management or through an on-site inspection.

Office manuals will help demonstrate the extent to which the policies and procedures are in place. Data on training and information on the method for detecting training needs will give information on the quality of AML/CFT training.

Data on the sanctions imposed on staff for failing to abide by AML/CFT breaches can give some useful indications on the implementation of AML/CFT defences, although the raw data are unlikely to be definitive without further inquiry.

Where a jurisdiction permits institutions to rely, to some extent, on the CDD undertaken by third parties, it will need to impose measures to mitigate the risks of such a practice. The FATF demands that FIs and DNFBPs should be able to obtain original CDD documentation from third parties without delay. It is good practice to require FIs and DNFBPs to test the ability of third parties to supply such information on a random basis. This provides some reassurance that the documentation will be available when required. It also avoids the risk that a request for information may amount to a form of tipping off that an investigation is under way. Data on the random tests undertaken by an institution can show that it is actually undertaking such tests and show how reliable third parties are in supplying data.

Data on refused business can show the extent to which an FI or DNFBP is considering the implications of a refusal to undertake business with a customer or other counterparty. This can indicate how serious the institution is in conducting its risk assessment of customers and reporting suspicions.

The supervisor may choose to impose additional specific reporting requirements on individual institutions on the basis of the risk scoring of institutions.

It is unlikely that a supervisor will wish to insist on all institutions submitting all of this information in every periodic report. A supervisor should not demand data that are then not analyzed and reviewed, since the data may reveal a problem that could become much greater at some future date and the supervisor will be rightly criticized if it is shown that the supervisor had indications from the relevant report but did not detect it. Whatever a supervisor asks for must be properly analyzed. The supervisor should choose which of the categories of information to ask for and may make a different decision for different institutions or different classes of institution.

The resources devoted to analyzing such reports can provide information that can refine the supervisor's understanding of the state of compliance by different institutions and thus target on-site inspections (which are even more resource intensive) more effectively.

The periodic reports are the most comprehensive set of regular data obtained on institutions, and it is important that they are used to adjust the risk scoring of each institution according to the supervisor's methodology.

Information from the FIU and market intelligence
The FIU has responsibility for receiving suspicious transaction reports. It, or some other law enforcement agency, may have responsibility for investigating them or for otherwise following up on allegations of ML or TF. These agencies can provide information on the effectiveness of reports filed by FI and DNFBPs. They can also provide information on the adequacy of the record keeping by FIs and DNFBPs as evidenced by their ability to supply information (for example about beneficial owners) and trace funds. This is valuable information about the state of compliance by FIs and DNFBPs with their AML/CFT obligations and the supervisor should find ways of obtaining this information consistent with the general requirement for the FIU to keep certain information about investigations confidential.

The supervisor's information about the development of the market – for example as a result of prudential and conduct of business supervision – can also provide information about the developing ML/TF risks in the market and the actions taken by FIs and DNFBPs to mitigate that risk. The supervisor should endeavour to ensure that it captures this information.

Themed third-party reviews and questionnaires
Many supervisors have the right to appoint third parties (such as audit or law firms or other professionals), or to require institutions to appoint such third parties to carry out specific investigations. This power can be used as an alternative to an on-site inspection. It can be particularly useful where there is a need to review the state of compliance with a particular aspect of the AML/CFT defences, such as the measures in place to detect if customers are PEPs or the measures to identify beneficial owners. Such themed reviews by third parties can, if properly commissioned, provide useful intelligence while conserving the use of the skilled manpower within the supervisory authority.

Similarly, a supervisor wishing to establish compliance with a particular aspect of the AML/CFT obligations can conduct a survey of institutions through the use of a well-structured questionnaire. This can be used, for example, to obtain data not supplied routinely through periodic reports.

On-site inspections
Inspections can be full scope – designed to determine the level of compliance with all aspects of the AML/CFT regime; can be themed – to establish the level of compliance with a particular aspect of the regime by all, or a number of, institutions; or can be targeted – to review a specific aspect of compliance by a specific institution. All are valuable uses of the inspection tool.

It is important for the supervisor to have the power to conduct inspections without cause or notice, although it will usually be more efficient to give notice.

The inspection program should be determined on the basis of the risk assessment of the supervisor and the risk scoring of all institutions. The selection methodology should take account of the time since the last inspection so that even the lowest-risk institutions are inspected at some stage. In principle, no FI or DNFBP should have a gap of more than four years between inspections, and for high-risk institutions the gap should be very much less.

Each inspection should be carefully planned by consulting information from periodic reports and previous inspections so as to define a set of objectives and issues that are specific to the inspected institution. It is not sufficient to rely on generic objectives as this does not make maximum use of supervisory intelligence. The objectives and issues should determine the approach and methodology of the inspection. The institution should be told which documents and files should be made available before and during the inspection, although some files should be demanded without notice, so as to test the institution's readiness.

The precise scope of an inspection will depend on the risk assessment and risk scoring, but it is likely that the supervisor will wish to focus at least in part on the governance of the institution. This will require an examination of board papers and interviews with management and non-executive directors. Otherwise, the supervisor is likely to want to test the quality of the risk assessment, and the nature of the policies and procedures – particularly customer acceptance policy and due diligence procedures, customer monitoring and review, reporting, training, controls, and staff screening.

The conclusions of the inspection should be communicated to the institution, a draft report submitted in reasonable time (no more than four weeks), and an action plan agreed with the institution with timetables and a reporting procedure. The reporting procedure should, where possible, be combined with the normal periodic reports required of the institution.

The supervisor's risk scoring of the institution should be updated in the light of the inspection.

Enforcement

The purpose of the inspection and other monitoring tools is to maintain good practice, rather than find and punish errors. Recommendations for action should be focused on systems, controls, and training rather than rectification of single breaches (although those found should be put right). The supervisor should seek to find the reasons for the error and correct those.

Sanctions should be a last resort, although it may be necessary to impose sanctions from time to time. The supervisor should seek to equip itself with a range of sanctions proportionate to the severity of the breaches. If the only sanction is to suspend or withdraw authorization, it is likely to be unusable except in extreme circumstances. The supervisor should seek to have a range of sanctions that include private and public written warnings, fines, the suspension or removal of specific officers (including the board and senior management), and the imposition of licence conditions – for example, restricting the nature of business until remedial measures are in place), as well as the suspension or revocation of authorization.

Implementing sanctions regimes for terrorist financing

The FATF is increasing its focus on measures to combat terrorist financing. It has published typologies and is likely to be publishing more guidance. Supervisors will need to keep abreast of developments in this area.

At a minimum, the supervisor will need to be aware of the main terrorist financing sanctions regimes and the way in which they should be implemented by FIs and DNFBPs. These regimes

are based on United Nations Security Council Resolutions (UNSCRs), for example 1267 (relating to Al Qaeda), 1988 (the Taliban), 1718 (North Korea), 1737 (Iran), 1373 (terrorism in general), and successors or updates to these resolutions. For all these UNSCRs, except 1373, the UN designates organizations and individuals subject to sanction.

It is mandatory on all countries that apply FATF Standards to apply these sanctions, which, in general terms, require FIs and DNFBPs to deny access to the financial system to the designated organizations and individuals. It is not mandatory on all countries to apply UNSCR 1373, but it is up to national authorities to designate organizations and individuals subject to sanction. Institutions and supervisors should be aware that persons designated by the US under UNSCR 1373 are particularly important. Because of the importance of the US dollar in international finance, many transactions, even if not apparently involving the US or US institutions, may, in practice, be subject to US jurisdiction due to a connection to US dollars at some point in the transaction chain. Many non-US FIs that use dollars (and most do) may consider it prudent to monitor and apply the terrorist designations made by the US.

The supervisor must be in a position to understand how its jurisdiction disseminates information on those subject to UN-designated sanctions and which organizations and individuals are designated by its own domestic authorities. The supervisor must then ensure that there is a mechanism for ensuring that all FIs and DNFBPs understand who is subject to sanction. Each FI and DNFBP must have a means of detecting if they have any such person as a customer, beneficiary, or counterparty. The FIs and DNFBPs must be able to deny anyone on the sanctions list access to finance.

The sanctions regime is not subject to the risk-based approach, in that it is a requirement that all FIs and DNFBPs should apply the sanctions.

Conclusion

This Note has emphasized the following key points about the supervision of AML/CFT obligations:

- the supervisory approach should be risk-based, starting with the National Risk Assessment and applying that to the supervisor's risk assessment of the business and the risk scoring of institutions;
- the risk-based approach applies to FIs and DNFBPs, which must be obliged to conduct a risk assessment of their business and identify the risks associated with each customer as the basis for the application of CDD measures;
- the supervisor's risk assessment should inform the use of all supervisory tools, including standard setting, authorization, raising awareness of obligations, and monitoring compliance with standards;
- all the available monitoring mechanisms should be used and not simply the on-site inspection; and
- a key focus of the supervisor's standard setting and monitoring should be the governance of the institution.

The supervisor is responsible for ensuring compliance with the FATF preventive measures. Although the FATF Requirements appear complex, it is important to focus on the core concepts

of customer identification and risk assessment, customer profile building, customer monitoring, and reporting.

FIs and DNFBPs must understand that AML/CFT risk mitigation is as much a part of the management function as the management of credit risk, market risk, customer asset risk, and all the other risks with which they are familiar. They should be guided to train their staff to see the AML/CFT defence as a logical process and not merely a series of arbitrary bureaucratic procedures involving placing passport photocopies on files. By adopting the risk-based approach and focusing on governance, the supervisor should be well placed to achieve this level of understanding by FIs and DNFBPs.

References

Alliance for Financial Inclusion. *Gender Considerations in Balancing Financial Inclusion and Anti Money Laundering and Countering the Financing of Terrorism*. November 2018. https://www.afi-global.org/sites/default/files/publications/2018-11/AFI%20GSP_laundering_stg7.pdf

Basel Committee on Banking Supervision. *Sound management of risks relating to money laundering and financing of terrorism.* Revised July 2020. https://www.bis.org/bcbs/publ/d505.pdf

Financial Action Task Force. *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing*. June 2007. https://www.fatf-gafi.org/media/fatf/documents/reports/High%20Level%20Principles%20and%20Procedures.pdf

Financial Action Task Force. *Concealment of Beneficial Ownership.* July 2018. https://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Egmont-Concealment-beneficial-ownership.pdf

Financial Action Task Force. *International standards on combatting money laundering and the financing of terrorism and proliferation.* The FATF Recommendations. Updated June 2019a. http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

Financial Action Task Force. *Virtual Assets and Virtual Asset Service Providers.* June 2019b. https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

Financial Action Task Force. *The Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CTF Systems*. Updated October 2019c. http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf

Financial Action Task Force. *Guidance on Digital Identity.* March 2020. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf

Toronto Centre. *Risk-Based Supervision*. March 2018. https://res.torontocentre.org/guidedocs/Risk-Based%20Supervision%20FINAL.pdf

Toronto Centre*. Risk-Based Supervision for Securities Supervisors (and Other Supervisors of Small Firms).* February 2020. https://res.torontocentre.org/guidedocs/Risk-Based%20Supervision%20for%20Securities%20Supervisors.pdf