RegTech at the Service of FATF Standards

Fatemeh Mahjourian Ghomi, Senior Officer, Central Bank of Iran,
f.mahjourian@cbi.ir

Abstract

Financial Action Task Force[1] is the most important body which is active in the field of Anti-Money Laundering and Combating Financing of Terrorism[2] and is a standard-setting body whose recommendations are widely accepted by countries. The history of its recommendations dates back to 1990 when the AML recommendations were introduced. Later, in 2001, the CFT recommendations were added and at present this group has got 40 recommendations covering AML, CFT and proliferation, which are observed by more than 200 countries.

Some of the recommendations of this group are the ones which should be observed by financial institutions and their non-compliance or non-effective compliance may expose the financial institutions to risks which would entail heavy penalties for them.

In the past, the financial institutions were trying to train their human resources in order to ensure compliance with international AML/CFT requirements; however, due to the crises which have taken place, now financial institutions seek assistance from technology; which ensures them that regulations would be observed more effectively.

In case technology is properly used, it can help financial institutions in the correct implementation of AML/CFT rules and regulations and increase their effectiveness in the areas including: on-boarding customers and customer due diligence, suspicious transaction reporting, risk-based approach, etc, which are all among the requirements set by FATF. Regulatory Technology[3] which is the result of the marriage of بِ technology پ and بِ regulations پ is trying to manage the compliance risk and decrease the ever-increasing compliance costs for financial institutions.

The purpose of this article is to review and study those FATF recommendations that RegTech can help financial institutions to comply with more than before.

[1] FATF
[2] AML/CFT
[3] RegTech

RegTech, FATF, Money laundering, Financing of terrorism, Customer due diligence, Suspicious transaction.

Introduction

The purpose of this research is to make closer ties between the technology providers who are offering technical tools to banks on one hand, and the banking sector who is the user of such services on the other hand. The gap which exists now is that technology providers know what they should include in their RegTechs without being aware what international standards they are exactly rooted in and without knowing whether they are applicable in the I.R. of Iran or not, and bankers know what they should comply with (international standards and local rules and regulations) without (maybe) knowing how IT can help them in this respect.

In this article, first we would review the FATF standards that banks should comply with and then we will discuss what RegTech can offer banks in order to assist them in carrying out their duties. Some may already be known to the technology providers; however, maybe some of these topics have remained untouched; while it would be easy for the world of technology to assist banks in those areas as well. Then there will be a matching between recommendations and RegTech services and Iranی rules and regulations in the field of Anti-Money Laundering and Financing of Terrorism will be also mentioned.

The author hopes that the kind of information which is being offered through this paper would help the technology providers to better understand and consequently present themselves to the banking sector by the kind of information they have about the international standards and the local applicable rules and regulations and thus sound more convincing and on the banking sectorی part, the common language would help them proceed with their developments more swiftly.

Literature

RegTech is a branch of Financial Technology [4]and is the technology which is available for helping the banking industry (and also other sectors) to comply with regulatory requirements and obligations. These requirements are mainly inspired by FATF recommendations and are reflected in local rules and regulations.

1. Financial Action Task Force:

FATF is an inter-governmental body which was established in 1989. The main purpose of its establishment was to combat the proceeds of drugs smuggling and later to combat proceeds of all serious crimes. In 2001 and only one month after 9/11 attack, the issue of combating terrorism financing was also added to their duties. In 2012, FATF reviewed its recommendation and issued the latest version of its recommendations which are 40 recommendations covering: AML, CFT and Proliferations.

FATF tries to figure out the risks and vulnerabilities which exist in different sectors/products, including banking sector, and then tries to manage and mitigate those risks through its recommendations. Its next stage is the assessment of the countries and jurisdictions to ensure that they comply with the recommendations and thus do not pose any threat to international financial stability. The supervisors of the countries have the duty to ensure that the obliged persons who are subject to the local rules and regulations (inspired by FATF standards) comply with the rules and otherwise they will be fined. There have been several cases where international banks have been fined for millions and billions of dollars due to non-compliance with money laundering and terrorist financing obligations.

The recommendations of FATF can be divided into 7 main categories: 1) AML/CFT policies and coordination, 2) Money laundering and confiscation, 3) Terrorist financing and proliferation, 4) Preventive measures, 5) Transparency and beneficial ownership of legal persons and arrangements, 6) Powers and responsibilities of competent authorities and other institutional measures, and 7) International cooperation. The list of recommendations is as follows:

[4] FinTech

1 - Assessing risks & applying a risk-based approach;

2- National cooperation and coordination;

3- Money laundering offence;

4- Confiscation and provisional measures;

5- Terrorist financing offence;

6- Targeted financial sanctions related to terrorism & terrorist financing;

7- Targeted financial sanctions related to proliferation;

8- Non-profit organizations;

9- Financial institution secrecy laws;

10- Customer due diligence;

11- Record keeping;

12- Politically exposed persons;

13- Correspondent banking;

14- Money or value transfer services;

15- New technologies;

16- Wire transfers;

17- Reliance on third parties;

18- Internal controls and foreign branches and subsidiaries;

19- Higher-risk countries;

20- Reporting of suspicious transactions;

21- Tipping-off and confidentiality;

22- DNFBPs: Customer due diligence;

23- DNFBPs: Other measures;

24- Transparency and beneficial ownership of legal persons;

25- Transparency and beneficial ownership of legal arrangements;

26- Regulation and supervision of financial institution;

27- Powers of supervisors;

28- Regulation and supervision of DNFBPs;

29- Financial intelligence units;

30- Responsibilities of law enforcement and investigative authorities;

31- Powers of law enforcement and investigative authorities;

32- Cash couriers;

33- Statistics;

34- Guidance and feedback Sanctions;

35- Sanctions;

36- International instruments;

37- Mutual legal assistance;

38- Mutual legal assistance: freezing and confiscation;

39- Extradition;

40- Other forms of international cooperation.

From among these recommendations, the chapter dealing with بPreventive Measuresپ (recommendation 9 to 23) is related to financial institutions and puts certain responsibilities on their shoulders. Due to the money laundering cases and terrorist activities and also global financial crises, at present financial institutions are, indeed, overloaded with a lot of reporting requirements. Considering the tough standards in place and the records of financial institutions being fined, the cost to manage these requirements has increased drastically. It is hoped that the use of RegTech can help financial institutions to manage and satisfy regulatory expectations and at the same time save costs.

2. RegTech

RegTech is the result of marriage of Technology and Regulations and its main goal is to manage compliance risk and find solutions for compliance regulatory challenges through modern technology. One of the main favors that RegTech does to banks is reducing their AML/CFT compliance costs. But it goes beyond that. Since the issues of AML/CFT and obligations to comply with sanctions lists are sensitive and can affect the legal and reputational risks of financial institutions, RegTechs can help in preserving such good reputation.

RegTech is usually referred to as the technology of digitization of manual reporting and the compliance processes, but in fact it can go far greater than that. Besides facilitating an efficient regulatory compliance, it is a real-time and proportionate system that creates a regulatory regime which identifies and addresses risk.

Arnet, d.w. (et al) define RegTech as بthe use of technology, particularly information technology[5], in the context of regulatory monitoring, reporting and complianceپ

RegTech can help financial institutions in different aspects, the most famous of which are as follows:

* Customer onboarding and maintenance;
* Client screening;
* Transaction monitoring and filtering;
* Reporting and management information[6];
* Risk assessment.

Each of these categories will be reviewed in more details.

2.1 Customer onboarding and maintenance

One of the ways to combat money laundering and terrorist financing is to know the customers well. Knowing the customer can lead to production of high quality suspicious transaction reports as well. Customer onboarding and maintenance are the two areas that technology has proved to be of great help by minimizing operational costs. Customer Due Diligence[7] which seems to be a subjective issue, by the help of technology is turning into a subject which deals with numbers. RegTech can help Know your Customer[8] process in the following ways:

2.1.1. Third-party data providers, which might be a specialist AML/KYC firm or a credit reference agency. Many financial institutions across the world use such services and find it quite essential in their daily work. The important point about this service is that the information should

[5] IT
[6] MI
[7] CDD
[8] KYC

be regularly updated; otherwise it would lead to inaccurate decisions about customers. The accumulation of this information helps financial institutions to better find trends and suspicious individuals/institutions and have a clearer view of the entire transactional profile of an individual across the country.

One criticism to this kind of services is that for Enhanced Due Diligence[9] cases and adverse media, the manual work is still inevitable and therefore one cannot fully rely on the technology. Financial institutions hope that technology advances in a way that there would be the least possible dependence on human operators. This is while some supervisors and regulators believe that technology can never be solely relied upon and the combination of human resources and technology always produces the best results.

2.1.2. The other service which is offered by RegTech is the use of biometrics in identification and verification of customers (in particular for customer maintenance purposes). By using information from multiple data sources, RegTech can reduce the amount of time it takes to onboard new customers. The biometrics services used for authentication of existing customers can be divided into 4 categories:

* Voice-based biometrics for telephone contact centers.

* Device-based biometrics for digital interactions with customers (especially the use of fingerprint scanning).This technology is quite economical and more secure in comparison with passwords. The advanced technology can also offer geolocation data from phones which can be helpful in better understanding the behavior and personal profiling of consumers such as understanding his/her usual locations, etc.

* Facial recognition technologies (or Video KYC) which is useful in environments when customers do not have access to branches (such as remote areas or in some emerging markets)

* Vein pattern recognition, which is used much less.

It should be noted that these services are usually used for easy access of customers to their accounts via digital and telephony channels. They can speed up KYC procedures by

[9] EDD

facilitating non face-to-face verification and by making it easier for customers who have limited credentials to access financial services and thus help financial inclusion.

2.2. Client screening

This service is usually required for screening the customers who are PEPs or whose names are mentioned in sanction lists or they are considered as high risk customers for any other reason. The names of customers are matched against the available databases.

For the financial institutions that are acting as a financial group with branches and subsidiaries in different jurisdictions, one of the problems are differences in languages. Complex names with different spellings pose real problems and technology can help with translation issues. The other area of difficulty for financial institutions in the client screening process is manual false positives reviews; advanced technology can help in this respect through analytics, machine learning and NLP. Some financial institutions also use the third party legal entity databases for identifying beneficial owners.

2.3 Transaction monitoring and filtering

This is an area that technology is helping a lot and there are still rooms for further advancements. Technology is used to monitor and filter transactions and prevent the transactions that might originate or target sanctioned countries, entities and individuals and tries to identify the transactions that have high risks. For the technology to be effective at this part, it should have certain features: accuracy, intelligence, speed and low cost.

Nowadays a lot of payments are made by mobiles and we are moving to a بcashless societyپ and this means that banks have to monitor more transactions. RegTech can help financial institutions to scale their screening effectively as trends in payments evolve.

It should be pointed out that this transaction monitoring and filtering can happen in post-event mode or as a real time analysis and the second status is definitely more favorable. Therefore the features of a successful technology in this field are: 1) to undertake real time analysis, 2) to produce less false alerts.

2.4. Reporting and management information

The production and filing of suspicious transaction reports can be done more effectively by the help of technology. RegTech can help sending automatic STRs to FIU without any manual control. This, of course, is recommended only in cases that Suspicious Transaction Reports[10] have been proved to be of very high quality. Many experts believe that combination of human resources capability with that of technology would enrich the process and provide a more fruitful result. Since the recipient of the STRs is Financial Intelligence Unit[11], it is very important that FIU, based on its policies and procedures and the technology it has in hand, would be ready to accept automatic STRs. The technology can also help in tracking the progress of STRs.

2.5. Risk Assessment

Robo advisors (which are methods to automate risk assessment via a computer algorithm) can help in having an adequate risk assessment and understanding the specific risk exposures. According to Comply Advantage team،ب They can also improve the quality of high risk decision-making by offering advice which has been gleamed from processing historical dataپ

Tables 1 and 2, which is extracted from the paper issued by PA Consulting Group on behalf of Financial Conduct Authority (2017) show the kind of technologies which might be used for AML purposes.

[10] STRs
[11] FIU

Technology	Description	Illustrative example of how it may aid AML compliance	Respondents' views: is it proven in practice?	Respondents' views: challenges to implementation
Biometrics	Using biometrics (including via mobile devices) such as fingerprints, iris recognition, vein mapping and voice recognition to identify customers.	Biometrics have particular promise in the customer onboarding and maintenance space – particularly for authenticating ongoing customer interactions.	Respondents felt that biometrics represented proven technology, although with a potential heavy reliance on mobile devices.	Respondents felt that the biggest challenge to implementation was around difficulties in securing the registration step when using mobile-device based biometrics.
Blockchain	Using distributed ledger-based database technology for a variety of potential use cases.	Blockchain has a variety of theoretical use cases in aiding AML compliance, with some of the most promising being in the transaction monitoring space.	Respondents felt that the technology was proven at a fundamental level - but there was widespread scepticism over whether the 'right' use case has been identified.	Respondents felt that there was a lack of compelling use case for the technology; the technology was considered opaque and 'hard to sell'.
Data Analytics and Machine Learning	Using advanced analytics and machine learning capabilities to process large volumes of data in an accelerated timeframe, with continuous improvement.	Analytics and machine learning have a number of different applications; many of the most promising involve using these systems for transaction monitoring for more complete analysis of unusual transactions, potentially in real time.	Respondents felt that analytics/machine learning were widely used and proven technology areas, albeit evolving constantly.	Respondents felt there was sometimes a lack of business case to move away from existing solutions, and that data quality remains a substantial limiting factor.
Geolocation	Using a customer's location data to determine a behavioural profile/support financial crime compliance activities.	Geolocation technology can be used in a multitude of ways, including: verifying a customer's location matches a recognised address, creating a behavioural profile for transaction monitoring purposes and more.	Respondents felt that the technology was proven, although noted that accuracy can vary by device.	Respondents felt that using and collating the device data in real time can be a challenge, as can the broader data privacy implications.

Table 1

Technology	Description	Illustrative example of how it may aid AML compliance	Respondents' views: is it proven in practice?	Respondents' views: challenges to implementation
Industry Utilities	Third-party service/technology providers offering the wholesale outsourcing of various compliance activities across a whole industry.	Industry Utilities were most commonly considered for CDD/ID&V purposes, although could theoretically work across the AML lifecycle.	Respondents felt that the technology was generally proven, although adoption in many geographies (including the UK) has been slow	Respondents felt there were a number of significant challenges to widespread adoption, including a lack of clear standards and low risk appetites meaning regulated firms were often unwilling to outsource these activities.
NLP	Natural Language Processing encompasses technologies that can mimic or analyse human speech/languages.	NLP has various AML compliance use cases; many of the more prominent relate to enhanced client screening capabilities, including name translation/ transliteration.	Respondents felt that the technology was broadly proven although still evolving. They felt that functionality was proven to a greater extent for more simplistic-tasks rather than full language replication/analysis	Respondents felt that the technology potentially lacks effectiveness in more complex areas of analysis, although noted this was continually evolving.
Video KYC	Performing KYC checks over a video link to enable remote gathering of information	Video KYC is perceived as allowing the benefits of in-person customer interactions without requiring a branch network, particularly for performing customer onboarding related compliance activities.	Respondents felt that Video KYC technology was generally proven.	Respondents felt that there was no broad desire for the functionality from consumers, no clear consensus on which underlying technology to use, and often minimal advantages over existing digital interactions.
Workflow Tools	Advanced workflow tools provide combination workflow, case management and MI tools to control and support various operational activities.	Workflow tools have a number of AML compliance use cases. Common uses include in customer onboarding to create a single KYC 'file' as well as in SAR production/analysis/reporting.	Respondents felt that the technology was both proven and readily available.	Respondents felt that it was often challenging to put forward a compelling business case, with other technologies perceived as providing greater tangible benefits, either in terms of financial crime prevention or cost reduction.

Table 2

Supervisors and RegTech

It is not only the financial institutions who need to use RegTech. Even regulators & supervisors, who have the challenge of regulating and supervising in such rapidly transforming financial systems, can use RegTech in order to fulfill their already existing responsibilities (like financial stability, prudential safety and soundness, consumer protection), and also the responsibilities in the field of AML/CFT compliance i.e. to identify the extent to which financial institutions are complying with AML/CFT requirements.. RegTech can also help supervisors to have an understanding of money laundering and terrorist financing risks. RegTech can help supervisors to demonstrate that their actions have an effect on compliance by financial institutions. The last point which should be made here is that regulators also have budget problems and RegTech can help them in a more economical supervision.

Research Method:

The purpose of this research was to see to what extent RegTech is at the service of FATF standards and can help banks in complying with those standards.

To achieve the answer to this question, the kind of services that RegTechs offer were reviewed. It should be noted that in some cases they relate to compliance requirements in general (which is beyond AML/CFT areas and cover financial crimes as well).

In the next step, the FATF recommendations were reviewed to see which ones are met by RegTech at present and which ones are possible to be met by RegTech in the future, to give food for thought to technology providers.

To collect the information, the library research process was used and the findings were matched against each other. In the last stage, to give a better view of the prospect which is ahead, the applicable domestic rules and regulations were also included.

Findings:

Customer onboarding and maintenance

Many IT technicians know that KYC and CDD are integral parts of the AML compliance; however, they may not be aware that where in the international standards it has been stipulated.

The issue of CDD is a key core recommendation, i.e. recommendation 10 of FATF. The recommendation reads as follows:

ِFinancial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names. Financial institutions should be required to undertake customer due diligence[12] measures when: (i) establishing business relations; (ii) carrying out occasional transactions: (i) above the applicable designated threshold (USD/EUR 15,000); or (ii) that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation

[12] CDD

16; (iii) there is a suspicion of money laundering or terrorist financing; or (iv) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The CDD measures to be taken are as follows: (a) Identifying the customer and verifying that customerپ identity using reliable, independent source documents, data or information. (b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer. (c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship. (d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institutionپ knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Financial institutions should be required to apply each of the CDD measures under (a) to (d) above, but should determine the extent of such measures using a risk-based approach[13] in accordance with the Interpretive Notes to this Recommendation and to Recommendation 1.پ

* Summary of the recommendation 10:

- when financial institutions should carry our CDD,
- how they should do it with an emphasis on the بon-goingپnature of CDD,
- the need to adopt Risk Based Approach to CDD,

CDD is the topic that RegTech can help Iranian financial institutions as well. Chapter 2 of the AML by-law and chapter two of the CFT by-law have made this obligations of financial institutions clear in this respect. RegTech can ensure financial institutions that they do not have any anonymous account (in Iran it means no account without national ID number).

[13] RBA

Establishing business relationship is the onboarding stage and carrying out CDD at the time of occasional transaction refers to the maintenance part of the RegTech responsibilities, as described.

At this stage there are some differences between the domestic rules and FATF standards that RegTech providers should take into account and that is the fact that for wire transfers and occasional transactions, no threshold is considered in Iran when identification and verification stage is to be carried out. The differences which exist between FATF standards and domestic rules and regulations can be the subject of another study, and only one case was mentioned here to attract the attention of technology providers to these delicate issues.

One of the services that RegTech offered for CDD was through بthird-party data providersپ It should be noted that based on recommendation 17 of FATF on بReliance on third partiesپ

بCountries may permit financial institutions to rely on third parties to perform elements (a)-(c) of the CDD measures set out in Recommendation 10 or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for CDD measures remains with the financial institution relying on the third party.

The criteria that should be met are as follows: (a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a)-(c) of the CDD measures set out in Recommendation 10. (b) Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay. (c) The financial institution should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements in line with Recommendations 10 and 11. (d) When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country riskپ

Although reliance on third parties has been permitted in FATF standards, however; considering the provisions of article 8 of AML by-law, it seems that this cannot be used in the Iranی financial system.

Client screening

Recommendation 12 on PEPs states that:

یFinancial institutions should be required, in relation to foreign politically exposed persons[14] (whether as customer or beneficial owner), in addition to performing normal customer due diligence measures, to: (a) have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person; (b) obtain senior management approval for establishing (or continuing, for existing customers) such business relationships; (c) take reasonable measures to establish the source of wealth and source of funds; and (d) conduct enhanced ongoing monitoring of the business relationship.

Financial institutions should be required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization. In cases of a higher risk business relationship with such persons, financial institutions should be required to apply the measures referred to in paragraphs (b), (c) and (d). The requirements for all types of PEP should also apply to family members or close associates of such PEPsپ

- Summary of Recommendation 12:

For 1) یforeign PEPS and 2) domestic PEPs & those who have been entrusted with a prominent functions by an Intلی organizationپand their family members and close associates, some extra due diligence measures shall be carried out.

Recommendation 6 also deals with sanction lists related to terrorist financing:

یCountries should implement targeted financial sanctions regimes to comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. The resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to

[14] PEPs

or for the benefit of, any person or entity either (i) designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) designated by that country pursuant to resolution 1373 (2001)پ

- Summary of recommendation 6:

- The names mentioned in resolution 1267 and its successors (i.e. Taliban, Al-Qaida and ISIS) should be included in the databases.
- Based on resolution 1373, each country should have its own national list whose names also should be included in the databases.

The issue of PEPS and sanctions lists was used as example of the cases for which be client screening should be carried out. The responsibility to screen PEPs also exists in Iran. Though domestic PEPs are covered by other regulations, foreign PEPs are covered in article 9 of the AML by-law and there is a separate directive on PEPs advised by the AML High Council to financial institutions; therefore this is the area that RegTech can help Iranian financial institutions.

For sanction lists, the Central Bank of Iran has been advising the names of Taliban and Al-Qiada (and later ISIS) for a long time and financial institutions shall ensure that they do not offer any services to the designated entities. Article 7 of the CFT by-law also makes it an obligation for the financial institutions to have tools and mechanisms which enable them identify the designated persons (national list under resolution 1373). In case of non-compliance, financial institutions will be punished.

Transaction monitoring and filtering

A part of recommendation 10 obliges financial institutions to:

بـ(d) Conduct ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institutionبـ knowledge of the customer, their business and risk profile, including, where necessary, the source of fundsپ

RegTech not only can establish rules that identify potentially criminal transactions, but it can train the system in a way that it can identify criminal transactions over time by analyzing a staggering array of factors. These could eventually come to include where a customer opens an account relative to their home address, what time of day an account was opened, duration between transactions, patterns among the merchants where a customer makes transactions, relationships between other customers of those same merchants, whether a customer uses a mobile telephone, what communication channel a customer uses to contact the bank and even changes in a customer's social media presence.

*** Reporting and management information (MI)**

The obligation to send suspicious transactions report is basically mentioned in recommendation 20 of FATF:

ب If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit[15] پ

Iran ی FIU is also established and its duties are described in article 38 of the AML by-law. Article 25 of this by-law obliges all financial institutions to send their STRs in confidentiality and without tipping off. RegTech can help the Iranian financial institutions in better performing such obligation.

*** Risk assessment**

Recommendation 1 of FATF deals with the issue of risk assessment and touches the issue at two levels: 2) national level, 2) obliged entities. The last part of recommendation describes the requirement as follows:

ب Countries should require financial institutions and designated non-financial businesses and professions[16] to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks پ

[15] FIU
[16] DNFBPs

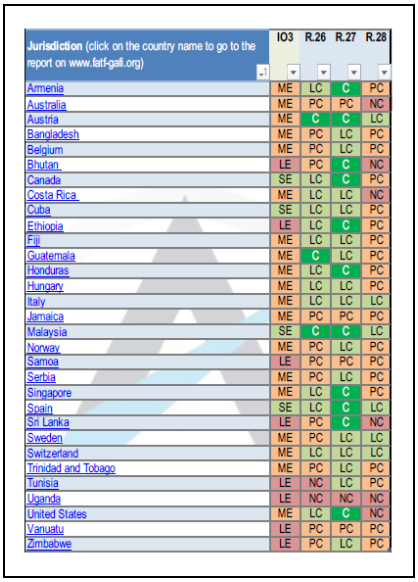
The necessity of having a risk-based approach has been reiterated in the CFT by-law and also in articles 3 and 4 of the Directive on KYC/CDD of Iranian Customers of Financial Institutions and thus, this is an area that Iranian financial institutions may benefit from RegTech.

Supervisors and RegTech

Based on FATF standards as mentioned in the document titled ؛Methodology for Assessing Technical Compliance with FATF Recommendations and the Effectiveness of AML/CFT Systems؛ supervisors are expected to supervise, monitor and regulate financial institutions for compliance with AML/CFT requirements, commensurate with their risks and provide financial institutions with adequate feedback and guidance. Over time, supervision and monitoring shall improve the level of AML/CFT compliance, and discourage attempts by criminals to abuse the financial sector, particularly in the sectors most exposed to money laundering and terrorist financing risks؛

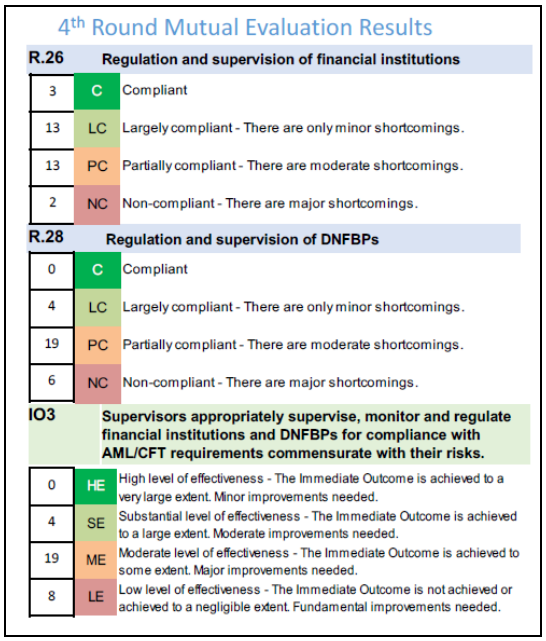
The analysis of the results of the 4th Mutual Evaluation Report[17] carried out by FATF on recommendation 26 (regulation and supervision of financial institutions) and 27 (powers of supervisors) of the countries which have gone under assessment indicates that supervisors have not been very successful in accomplishing their tasks (table 3). The terms used in table 3 are elaborated in Table 4.

[17] MER



Jurisdiction (click on the country name to go to the report on www.fatf-gafi.org)	IO3	R.26	R.27	R.28
Armenia	ME	LC	C	PC
Australia	ME	PC	PC	NC
Austria	ME	C	C	LC
Bangladesh	ME	PC	LC	PC
Belgium	ME	PC	LC	PC
Bhutan	LE	PC	C	NC
Canada	SE	LC	C	PC
Costa Rica	ME	LC	LC	NC
Cuba	SE	LC	LC	PC
Ethiopia	LE	LC	C	PC
Fiji	ME	LC	LC	PC
Guatemala	ME	C	LC	PC
Honduras	ME	LC	C	PC
Hungary	ME	LC	LC	PC
Italy	ME	LC	LC	LC
Jamaica	ME	PC	PC	PC
Malaysia	SE	C	C	LC
Norway	ME	PC	LC	PC
Samoa	LE	PC	PC	PC
Serbia	ME	PC	LC	PC
Singapore	ME	LC	C	PC
Spain	SE	LC	C	LC
Sri Lanka	LE	PC	C	NC
Sweden	ME	PC	LC	LC
Switzerland	ME	LC	LC	LC
Trinidad and Tobago	ME	PC	LC	PC
Tunisia	LE	NC	LC	PC
Uganda	LE	NC	NC	NC
United States	ME	LC	C	NC
Vanuatu	LE	PC	PC	PC
Zimbabwe	LE	PC	LC	PC

Table 3



4th Round Mutual Evaluation Results

R.26		**Regulation and supervision of financial institutions**
3	C	Compliant
13	LC	Largely compliant - There are only minor shortcomings.
13	PC	Partially compliant - There are moderate shortcomings.
2	NC	Non-compliant - There are major shortcomings.
R.28		**Regulation and supervision of DNFBPs**
0	C	Compliant
4	LC	Largely compliant - There are only minor shortcomings.
19	PC	Partially compliant - There are moderate shortcomings.
6	NC	Non-compliant - There are major shortcomings.
IO3		**Supervisors appropriately supervise, monitor and regulate financial institutions and DNFBPs for compliance with AML/CFT requirements commensurate with their risks.**
0	HE	High level of effectiveness - The Immediate Outcome is achieved to a very large extent. Minor improvements needed.
4	SE	Substantial level of effectiveness - The Immediate Outcome is achieved to a large extent. Moderate improvements needed.
19	ME	Moderate level of effectiveness - The Immediate Outcome is achieved to some extent. Major improvements needed.
8	LE	Low level of effectiveness - The Immediate Outcome is not achieved or achieved to a negligible extent. Fundamental improvements needed.

Table 4

Therefore supervisors (including Central Bank of Iran) may also give it a though about using RegTechs in performing their duties. Article 20 of the AML by-law has defined the

supervisors and has mentioned their duties i.e. to report whether obliged entities comply with rules and regulations or not.

Conclusions:

The services that RegTechs offer throughout the world are mainly rooted in the FATF standards. Some of such services may be offered to Iranian financial institutions as well since those recommendations are reflected in domestic rules and regulations. Some of those services cannot be offered since they are forbidden in the law or the infrastructure needed for tem is not available. There are other recommendations and domestic rules and regulations which pose problems for banking sector and this sector should cooperate closely and have dialogue with technology providers so that they may together find solutions for such problems.

References:

English

[1] Arner, W. (*et al*) (2016). *FinTech, RegTech and the Reconceptualization of Financial Regulation*, Northwestern Journal of International Law and Business.

[2] ComplyAdvantage team (2017). 5 Ways RegTech will Advance in 2017. https://complyadvantage.com/5-ways-regtech-will-advance-2017/

[3] FATF (2012), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, updated October 2016. France. PA Consulting Group on behalf of

[4] FATF (2013). *Methodology for Assessing Technical Compliance with FATF Recommendations and the Effectiveness of AML/CFT Systems.* France.

[5] Financial Conduct Authority (FCA) (2017). *New Technologies and Anti-Money Laundering Compliance*.https://www.fca.org.uk/publication/research/new-technologies-in-aml-final-report.pdf

[6] Petrasic, K. (et al) (2017). *The Emergence of AI RegTech Solutions for AML and Sanctions Compliance.* Risk and Compliance e-magazine.

فارسی:

مهجوریان، ف. (۱۳۰٦). دغدغه ناظران: فین تک از نگاه ناظران مالی فرصت است یا تهدید. پرونده ویژه مجله تجارت فردا.