

Conference Paper

Specifics of Compliance-Functions Application in the Sphere of AML/CFT

Komissarova D. A.¹, Myasishcheva E. R.¹, Potekhina V. V.¹, and Kabanova N. A.²

¹Financial University under the Government of the Russian Federation, student of the Faculty of Risk Analysis and Economic Security, Moscow, Russia

²Financial University under the Government of the Russian Federation, Candidate of Economic Sciences, Ph.D., Moscow, Russia

Abstract

In the article, the authors consider issues of AML/CFT implementation in a world and Russian practice as a global threat to the national security of states and the world community as a whole. Despite the existence of regulated AML/CFT systems in foreign countries, the events of recent years have shown the necessity for their modernization in accordance with the conditions of global realities. At the same time, domestic experience is reflected in the insolvency of AML/CFT requirements.

One of AML/CFT tools is the implementation of compliance functions in the activities of organizations. The authors carried out a complex analysis of the compliance phenomenon in Russian reality, identified and analyzed the main problems of introducing the function studied.

Keywords: AML/CFT, compliance function, compliance officer, regulator, credit and non-credit financial organizations, compliance risk.

1. Introduction

Global money laundering transactions are estimated at 2 to 5% of global GDP (roughly U.S. \$1-2 trillion annually). According to the United Nations Office on Drugs and Crime, authorities currently seize less than 1% of global illicit financial flows.

With the rising visibility of terrorist attacks, money laundering and terrorist financing are escalating as priority issues for governments across the globe. Over the last few years, in the U.S. alone, nearly a dozen global financial institutions have been assessed fines in the hundreds of millions to billions of dollars for money laundering and/or sanctions violations.

Corresponding Author:

Komissarova D. A.
 komis-dasha@yandex.ru

Received: 11 December 2017

Accepted: 20 January 2018

Published: 13 February 2018

Publishing services provided by
 Knowledge E

© Komissarova D. A. et al. This article is distributed under the terms of the [Creative Commons Attribution License](#), which permits unrestricted use and redistribution provided that the original author and source are credited.

Selection and Peer-review under the responsibility of the FinTech and RegTech: Possibilities, Threats and Risks of Financial Technologies Conference Committee.

OPEN ACCESS

2. Material and Theoretical Bases of Research

Currently, AML/CFT entities are organizations that provide any financial transactions, including credit organizations, non-credit financial organizations and charity foundations.

These companies have difficulties in implementing requirements in the research sphere, including the lack of a methodological basis for the mechanism of identification and suppression of questionable transactions.

The cost of compliance with AML/CFT requirements is quite high. According to new figures from WealthInsight, global spending on AML compliance is set to grow to more than \$8 billion by 2017 (a compounded annual growth rate of almost 9%). However, many balks at increasing compliance spend notwithstanding the cost of enforcement actions and large-scale penalties resulting from compliance failures. (Anti-Money Laundering // PWC URL: <https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey/anti-money-laundering.html> (date of the application: 01.11.2017))

Increasing threats that affect the stability and security of transnational organized crime have prompted the international community to organize a global system to counter money laundering and the financing of terrorism.

The activities of relevant international and regional AML/CFT organizations and structures are aimed at the development and implementation of international standards to combat money laundering and the financing of terrorism, the regulation of international cooperation in this field and the implementation of technical assistance programs.

The main international legal acts in the field of AML/CFT are the Council of Europe Convention on Laundering, Search, Seizure, Confiscation of the Proceeds from Crime and Financing of Terrorism of 01.05.2008 and the Directive (EU) of the European Parliament and the Council of the European Union on the Prevention of the Use of Financial systems for the purposes of money laundering or the financing of terrorism of 20.05.2015.

Speaking about the Russian legislation, the basic normative document regulating the research sphere is the federal law №115. (Federal Law of 07.08.2001 N 115 "On countering the legalization (laundering) of proceeds from crime" // Rossiyskaya Gazeta) According to this document, organizations are obliged to inform the Central Bank and Federal Financial Monitoring Service about all transactions subject to mandatory control, in particular about individual transactions for an amount equal to or exceeding 600

thousand rubles. In addition, mandatory control to the purchase and sale by individuals by cash in foreign currency or the acquisition of securities for cash, or the receipt of money under a bearer's check issued by a non-resident, and the exchange of banknotes of one denomination with banknotes of another denomination.

For non-compliance or violation of the AML/CFT legislation, fines could be to 50 thousand rubles for physical persons and up to 400 thousand for legal entities. In some cases, the suspension of the organization's activities for up to 60 days may be designated as a punishment. Nevertheless, the greatest damage to the organization can cause reputational risk, which will inevitably lead to an outflow of customers. Preservation of former clients and volumes of business will be impossible, since this type of activity is personalized, in which it is necessary to maintain a high level of own reputation.

It is worth noting that the domestic practice of applying legislation in recent years has led to an increase in the number of fines and revocation of licenses, both for credit and non-credit financial organizations. According to the statistics of the Central Bank, as of 01.01.2015, 86 banks have lost licenses, 33 of them for conducting questionable transactions, i.e. money laundering. Banks are sanctioned for violating Article 15.27 of the Code of Administrative Offenses of the Russian Federation "Failure to comply with the requirements of legislation on combating money laundering and financing of terrorism". According to experts, this is related most often to violations, because of which the necessary data were not transferred to authorized bodies or were transmitted late.

Such trends in recent years in the banking and NFO sectors motivate companies to take precautionary measures with regard to violations of AML/CFT legislation. One of the tools to prevent and reduce AML/CFT risks for companies is the organization and use of compliance functions is a system of internal corporate prevention of violations of AML/CFT legislation.

In Russia, the term appeared with the arrival of large foreign companies on the market, where this function is an integral part of the activity. The main goal is to minimize legal and reputational risks arising from violations of professional and ethical standards.

However, in Russian practice there is no coherent definition of compliance. In the financial structures of the Russian Federation, compliance is most often understood as an official who is responsible for compliance with internal control rules and special programs in order to counteract money laundering and terrorist financing.

In a letter from the Basel Committee on recommendations on banking supervision, compliance control is a banking supervisory authority that must ensure that an effective policy and compliance risk management procedure is applied in the bank, and the bank's management takes the necessary corrective measures when identifying compliance deficiencies.

In this paper, the term "compliance" is considered through AML/CFT and is defined by the authors as working with external third parties (counteragents, customers, partners and supervisors) in terms of identifying, updating data, as well as conducting activities to assess and reduce risks in activities of a company. In this case, compliance control is aimed at creating a reliable "foundation" for the organization, stable operating conditions.

A specific of the implementation of the function being studied in Russia is that compliance is mandatory for banks from the Central Bank of Russia, Federal Financial Monitoring Service and the Assay Chamber, which ensures the control of standard procedures.

Some of the functions of these supervisory bodies are also shifted to self-regulating organizations, which are some kind of mechanism that guides organizations to form compliance functions themselves, showing them the necessity and importance of this structure.

Legislation (Federal Law 01.12.2016 No. 315 "On Self-Regulating Organizations" // Rossiyskaya Gazeta) gives SROs various powers, both control and law-making. SROs advise their members on organization of special internal control, as well as conduct certification of AML / CFT specialists. In exercising their supervisory powers, SROs develop an impact system for those members who have committed wrongdoing in their activities. These include the mechanism of disciplinary proceedings against its members, the application of which can lead to public warning, fine or exclusion from SROs.

Analyzing the current practice of the banking sector, it is worth noting that two approaches are used for the implementation of the compliance function: the first approach is compliance with the law. The second one is based on the analysis of risks, where an own compliance organization is created, which includes not only compliance with the requirements of the law, but also own compliance and risk management mechanisms. (Krupyshev D. Risk Compliance Management in a Russian Bank. The competitive advantages of the system approach // Legal Insight)

Compliance risk is understood as application of legal sanctions or regulatory sanctions, significant financial loss or loss of reputation by the bank as a result of non-compliance with laws, regulations, standards of self-regulatory organizations or codes of conduct relating to banking activities (in accordance with the recommendations of the Basel Committee on Banking Supervision). It is worth noting that such risks are necessarily present, to some extent, in the activities of any organization.

However, most of the above-mentioned AML/CFT entities do not properly implement the compliance function, as banks do, and face compliance risks, although work is in progress in this direction.

The peculiarity of introducing and building compliance is a systematic approach that allows structuring and creating an effective function of ensuring compliance with legislative requirements in organizations of any type. The key issues are:

- an approach to identifying areas of compliance and methodology for constructing the compliance function;
- a structuring of compliance function (centralized and decentralized compliance function, division of responsibility areas with risk management function, internal control, internal audit);
- an external evaluation of the compliance function (who assesses the compliance function for what and what actions should be taken in this regard in the company).

More effective management of work processes occurs as organizations build:

- a reliable compliance process, reducing reputational risks and facilitating work with international counterparties by following the leading world practices;
- an integration of business into the global economy;
- the principle of fairness in the relations between market participants, minimization of corruption, financial, legal and reputational risks

According to generally accepted international practices, the compliance function in AML/CFT should be based on the following elements:

1. The existence of internal regulatory documents for the implementation of AML/CFT compliance functions, including policies in this area, internal procedures and the use of controls, and the existence of internal control rules (it is necessary to regulate procedures for verifying customer identification, submitting necessary reports by external control bodies, data archiving, compliance with licensing

requirements, the procedure for responding to requests of law enforcement agencies, as well as appeals to them).

2. The presence of a compliance officer - an employee with the authority and responsibility for compliance with all internal regulatory documents in the field of AML/CFT, for the modernization and development of compliance functions, for proper reporting (qualitatively, on time and on the basis of requirements); for creating conditions for the implementation of the training program for employees.
3. A balanced continuous training program for staff (the main objectives of this program are to explain and intervene AML/CFT policies and procedures, as well as training in basic methods and tools for identifying, localizing and preventing suspicious activity).
4. Regular monitoring and modernization of the components of compliance functions (timely stress testing of implementation of compliance functions, the introduction of new AML/CFT instruments, monitoring activities to assess the effectiveness of all relevant persons performing their duties, continuous improvement of the implementation of compliance functions).

3. Results

When implementing compliance functions, Russian companies face a number of problems. First, this is the fact that there are many different methodological approaches to the definition of this term, and, consequently, to identify the main goals and objectives of implementing the compliance approach in the company's activities. The lack of clearly defined limits of the compliance officer's work and the setting of different tasks for him (even within one organization) leads to inefficiency of his activity, duplication of functions of employees of other divisions, which is unacceptable for companies in the economic crisis. As a result, most Russian companies either do not implement the compliance function (especially in the AML/CFT sphere) or oblige other structural divisions to deal with its individual elements. Accordingly, in the first case, the company consciously assumes the risk of corresponding consequences, which could be avoided if the compliance function is complied with; in the second case, the unity of the approach to the implementation of this function within the company is lost, which leads to its less effectiveness.

Another no less important problem is the lack of highly qualified personnel who could implement and support the implementation of compliance functions within the organization. At the same time, specialists who have received significant foreign experience in this area are now "expensive" in the labor market and not all companies are ready to cooperate with them.

An unbalanced system of sanctions and control over violations of AML/CFT legislation is also a problem. Often, companies are much more profitable simply to pay a fine, rather than build a complex system with the introduction of compliance functions. Against the backdrop of the company's general operating system, violations in the AML/CFT enforcement regulations may be lost (since they contain certain specific forms of manifestation that must be purposefully identified). Thus, Russian companies operate on the principle: «they cannot notice, but if they do, we will pay a fine».

4. Conclusion

It is hard to say how much compliance systems are effective now. Despite the fact that the country's banks already have some experience in this function, other companies (including NFOs) do not have such experience, which is a significant problem. The system of implementation of the compliance function requires significant expenses for the maintenance of staff and the introduction of new software products. At the same time, it is quite difficult to assess the damage from implementation of compliance risks. All this happens because of the reactive and proactive approach in the work of compliance officers. Their task is to prevent losses from implementation of compliance risks. In fact, the final price of the consequences of the implementation of a particular risk is not known, which complicates the calculation of the effectiveness of the implementation of compliance functions.

However, banks need to act according to the recommendations of the mega-regulator, while issues related to the spread of compliance in other sectors of the economy (not just banking) without additional state intervention remain open.

References

- [1] Anti-Money Laundering // PWC URL: <https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey/anti-money-laundering.html> (date of the application: 01.11.2017).

- [2] Federal Law of 07.08.2001 N 115 "On countering the legalization (laundering) of proceeds from crime" (date of the application: 02.11.2017).
- [3] Federal Law 01.12.2016 No. 315 "On Self-Regulating Organizations" (date of the application: 02.11.2017).
- [4] Krupyshev D. Risk management in the Russian bank. Competitive advantages of the system approach Risk management in the Russian bank. Competitive advantages of the system approach // Legal Insight.