Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 169 (2020) 380–387

Procedia Computer Science

www.elsevier.com/locate/procedia

Post proceedings of the 10th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2019 (Tenth Annual Meeting of the BICA Society)

Contemporary approaches to money laundering/terrorism financing risk assessment and methods of its automation in commercial banks.

Sofya Klimova[a], Nazerke Zhampeiis[b] and Asmik Grigoryan[c]

[a, c]MEPHI, Kashirskoye shosse 31, Moscow, Russia
[b]EAG Secretariat, Staromonetniy lane, 31/1, Moscow, Russia

Abstract

The risk-based approach to anti-money laundering and combating terrorism financing (hereinafter - AML/CFT) came to the forefront in the FATF Recommendations updated in 2012.

According to the FATF Recommendation 1, commercial banks, which are an essential part of AML/CFT system, are required to identify, assess and take measures to mitigate their money laundering/terrorism financing (ML/TF) risks. It should be mentioned that banking practice consider the following types of ML/TF risks: inherent in a banking product (product risk); inherent in a client (client risk); inherent in a financial institution (in particular a commercial bank) and determining its possible involvement in suspicious transactions.

This article is devoted to contemporary approaches of such risks assessment and methods of its automation in commercial bank. Prompt preparation of risk reports in this area will allow the bank's risk management to take timely measures to neutralize emerging threats and vulnerabilities.

Keywords: AML/CFT, risk assessment, commercial banks, information technologies.

In 2012, the FATF issued a new edition of 40+9 Recommendations. This document highlights the risk-based approach to AML/CFT.

It worth mentioning, that the Central Bank of Russia was one of the first organizations which worked out recommendations for commercial banks to comply with the FATF's risk-based approach requirements. The title of

10.1016/j.procs.2020.02.233

the document is "Requirements to the Internal Control Rules of the Financial Institution for the Purposes of Counteraction to Legalization (Laundering) of Criminal Proceeds and Financing of Terrorism" dated March 2, 2012.

Another document that will be considered in this article is the Wolfsberg Group's Methodical recommendations on ML/TF risk assessment issued in 2015 (hereinafter Wolfsberg Group's recommendations). This document also focuses on the risk-based approach in the AML/CFT.

A comparative analysis of these two documents will allow us to see the changes in the ML/TF risk assessment approaches that happened over the last seven years.

Unlike the Bank of Russia, the Wolfsberg Group's approach considers 3 phases of ML/TF risk assessment and highlights categories such as inherent and residual risk (see Figure 1).

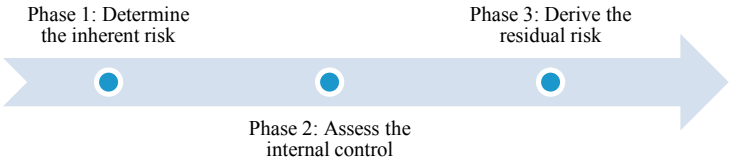

Figure 1. Risk assessment phases in line with Wolfsberg Group's recommendations

According to this approach, in the first phase bank should consider all relevant inherent risk factors such as clients, products and services, channels and geographies in order to determine its risk profile. Once the inherent risks have been identified and assessed, internal controls must be assessed to determine how effectively they can mitigate the overall risks. Available internal controls are evaluated for their effectiveness in mitigating the inherent ML/TF risk and to determine the residual risk rating.

Once both the inherent risk and the effectiveness of the internal control environment have been assessed, the residual risk can be determined. Residual risk is the risk that remains after controls are applied to the inherent risk. It is determined by balancing the level of inherent risk with the overall strength of the risk management activities and controls. The residual risk rating is used to indicate whether the ML risks within the bank are being adequately managed. [2]

Thus, the Wolfsberg Group proposes to assess the risk inherent in a commercial bank not only on the basis of such factors as customers and services (products), but also to adjust its level taking into account the assessment of vulnerabilities of the bank, namely, the quality of internal control tools used for AML/CFT purposes in each area of banking activity. Comparative analysis of the two approaches is given in Table 1.

Table 1. Comparative analysis of ML/TF risk assessment approaches of the Russian Central Bank and the Wolfsberg Group

	The Bank of Russia	**The Wolfsberg Group**
Number of risk assessment phases	1	3
Inherent risk assessment	+	+
Internal risks assessment and internal control instruments assessment	**-**	**+**
Residual risk assessment	**-**	**+**
Factors that affect inherent risk: - clients - products and services - geographies -other	 + + + -	 + + + +

In order to assess the quality of AML/CFT internal control policy implementation in each banking activity, we propose to use the following two groups of indicators.

The first group of indicators assesses the degree of involvement of a particular banking area in ML/TF suspicious

operations. In order to identify high-risk banking services and products for a particular financial institution, the following formula is proposed:

$$SST = TVT/GVT \quad (1)$$

Where,
SST - share of suspicious transactions in the whole volume of transactions is counted for each banking activity;
TVT - total volume of suspicious transactions of a particular type of banking services in the reporting period (RUB);
GVT - gross volume of all transactions conducted of a particular part of banking services (RUB).

In addition to this indicator, it is possible to assess the quality of the client's base in order to assess the bank exposure to the money laundering and terrorism financing risk.

The following figure is proposed for this purpose:

$$QCB = NSK/NC, \quad (2)$$

Where,
QCB - quality of client's base (%);
NSK - number of clients, whose transactions were qualified as suspicious in the reporting period (units),
NC - number of clients serviced in the reporting period.

At the same time, it seems reasonable to calculate this indicator separately for individuals, legal entities and individual entrepreneurs. Money laundering and terrorism financing risk is assessed based on the aggregate assessment of product risk and customer risk. Such a factor as banking services and products affects to money laundering risk in conjunction with the factor "internal environment", along with the factor "clients". In this regard, in order to identify the types of banking services subject to money laundering risk, it is also necessary to assess the quality of internal control programs for AML/CFT purposes implemented by the relevant departments of the bank.

The second group of indicators may be used to assess the quality of AML/CFT compliance. For this purpose, we propose to use a system of key risk indicators. In the process of monitoring and evaluating the level of operational risk, banking institutions around the world actively use indicators such as Key Risk Indicators (hereinafter - KRIs). Using the system of such indicators, the bank risk management is able to forecast unfavorable events and prevent them. Depending on the country's AML/CFT model, the KRIs may change. As an example, let us give the KRIs system, which can be used to assess the quality of implementation of the main requirements of the Russian anti-money laundering and combating terrorism financing legislation.

In essence, each indicator reflect the quality of each of the AML/CFT legal requirements implementation.

Table 2

Key indicators system for assessment of the quality of internal control procedures for AML/CFT Indicator name	**Total number of violations**	**Share in the total amount of violations in a bank**	**Share of violations attributable to i-th department of a bank**
I. Violation of internal AML/CFT control			
1. Number of violations of identification requirements.	…	…	…
2. Number of violations of staff training program and qualification requirements.	…	…	…
3. Number of violations of storage of information.	…	…	…

4. Number of facts of unreasonable submission of information to the FIU (financial intelligence unit)	…	…	…
II. Violations of obligatory control procedures			
1. Untimely submission of information on transactions (deals) which are the subject of control to the authorized body.	…	…	…
2. Submission of inaccurate information on transactions (deals) which are the subject of mandatory control to the authorized body.	…	…	…
3. Failure to submit information on transactions (deals) subject to mandatory control to the authorized body.	…	…	…
4. Violations of combating financing of terrorism and proliferation	…	…	…

In order to assess the share in the total number of violations in the bank as a whole, we propose to use the following figure:

$$STNV = NB / N \tag{3}$$

Where,
STNV – share in the total number of violations in a bank (%);
N – number of violations;
NB – number of violations of key indicator in the bank as a whole.

In order to assess the share of violations attributable to the i-th division of the financial institution, we propose to use the following figure:

$$STNV\_i = N\_i / N \tag{4}$$

Where,
i=1
STNV_i – share of violations attributable to the i-th division of the financial institution (%);
N – number of violations;
N_i – number of violations of the key indicator in the i-th division.

In order to assess the value of all indicators, it is proposed to use the following unified figure:

$$KRI = \Sigma N\_i * T\_i \tag{5}$$

Where,
i=1
KRI – total value of the Key Risk Indicator;
N_i – number of violations;
T_i – correction factor, which may differ, it depends on the severity of the violation and its consequences for the bank.

The proposed system of key risk indicators will make it possible to determine which areas of the credit institution are exposed to operational risk in the area of AML/CFT, as well as to develop an appropriate list of control procedures to adjust the risk level. The results of inspections of the internal control service can be used as a source of such information. It is proposed that credit organizations determine the frequency of updating information on their own, based on the needs

of the business. In order to ensure the representativeness of the obtained calculated data, it is advisable to collect and register data at least once a quarter.

We propose to apply BI-technologies as part of the automation of obtaining indicators used to assess the quality of the implementation of the internal control policy on AML/CFT in each banking activity.

Business intelligence (BI) is an advanced analytic software for business analysis and reporting. Most Business intelligence tools are used to access, analyze, and generate reports on data that is most often located in a data warehouse, data marts, and operational data warehouse. Application developers use BI platforms to create and implement BI applications. These programs can use data from various sources of information and provide them in a convenient form and section. Microsoft, SAS Institute, Oracle, SAP and others, represents this category of BI tool products.

As a rule, commercial banks use one or more different types of applications that satisfies the needs of bank's functions. There is a need to collect data from all source systems and integrate them into the data warehouse for developing the data warehouse as part of the BI system. Figure 2 presents a scheme of this process with subsequent receipt of BI results.

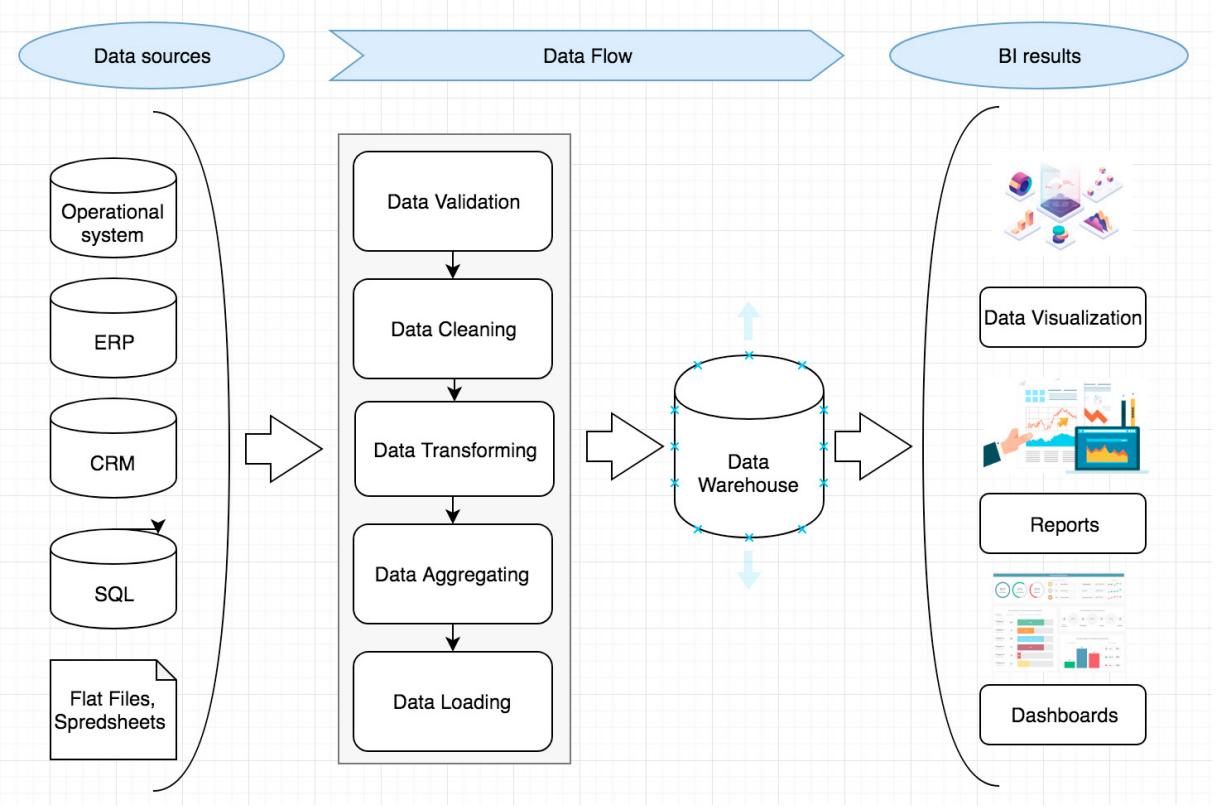

Figure 2. BI Scheme

The calculation of the indicators can be done using SQL queries to the database containing information about TVT, GVT, and NSK, NC as well as information from table 2 on the key indicators for assessing the quality of the implementation of internal control procedures for AML/CFT/CPF.

The results of SQL queries is the basis of an analytical report formation. It includes a group of indicators related to the assessment of the risk of legalization inherent in a certain type of banking service or a specific product (SST), and indicators to assess the quality of client's base (QCB).

It is very important to understand how to update data to get accurate results. It is necessary to request basic data sources for updating data, and then update all visualizations in reports or dashboards based on the updated data set. This procedure can be performed using a BI tool that satisfies the needs of bank's functions.

It is necessary to monitor the current state of the key indicators of risk assessment in commercial banks at least once a quarter and to consolidate responsibilities for each of the banking divisions involved in banking operations and transactions to ensure the relevance of the data in the reports.

The automation of the calculation of these indicators using BI technologies in commercial banks will allow identifying their own AML/CFT risks and taking measures to reduce them. The implementation of this approach does not require large financial and time costs, and positively affects the efficiency of the banking management system as a whole.

References

[1] Regulation of the Bank of Russia No. 375-P (2012) "Requirements to the Internal Control Rules of the Financial Institution for the Purposes of Counteraction to Legalization (Laundering) of Criminal Proceeds and Financing of Terrorism" (with amendments and supplement).

[2] The Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption.

[3] R.V. Zhubrin, (2010) “Combating money laundering (foreign and Russian experience)”. Monograph. – 316.

Instructions to Authors for Word template

1. Locking of Copyright:

The copyright line is locked in the Procedia templates. The author may not edit the same and making it editable only PSMs. If there are any copyright changes required, you are requested to contact Journal Manager through Guest Editors. For editable the below mentioned steps must be followed:

Steps:

- Click on copyright statement
- Click on **Properties** in **Developer** tab
- Remove the checks from **Content control cannot be deleted** and **Contents cannot be edited** under **Locking** and then Press **ok**

2. Docm format:

We have added macros in the Word templates for the below mentioned features. And since macros are not supported in doc and docx format we created the templates of all Procedia titles in .docm format.

- Removal of all highlights
- Accept track change
- Locking of Rules

If .docm format needs to convert in docx format then the following steps must be performed:

Steps:

- Press **Alt F11**
- Click on **Project (JID_Template)**
- Enter "thomson" in Project Password
- Click on Microsoft Word Objects
- Click on **ThisDocument** under **Microsoft Word Objects**
- Delete all macros under **General**
- After deletion close the **Code** and **Project (JID_Template)** windows
- From **File** menu click on save as type **.docx** option

3. Comments added in the margin in Word master templates:

There are instances where author raising queries on what to do with key information lines such as “volume, page numbers”, “Conference title per issue” and “Copyright entity, year, copyright company Elsevier Ltd./B.V./Inc. and Organizer Name” in the copyright statement and for these concerns the comments have been inserted in the Word template to guide Author/JM about the information to be inserted by them in these fields.

Comments removal from Print: In Word 2007 and 2010 the comments present in a document get printed by default. If the authors do not want to get the comments appearing in print, the authors must remove the comments from the Word template before printing by changing the Print markup setting of word using the following steps:

Steps:

- Click the **File** tab
- Click **Print**
- Under **Settings**, click the arrow next to **Print All Pages**
- Click **Print Markup** to clear the check mark

Instructions to Authors pages to be excluded from Print:

- Click the **File** tab
- Click **Print**
- Under **Setting**, Type page numbers and/or page ranges separated by commas counting from the start of the document or the section. For example, type 1, 3, 1-5

4. PDF creation from Word master template:

While creating PDF from Word template the below given steps should be followed to avoid difference in trim size and margins and to avoid decrease in resolution and size of the figure images of the Word template and the PDF created.

Steps in Word 2007 and 2010:

- Click the **File** tab
- Click **Print**
- Under **Printer** tab, select **Adobe PDF**
- Click **Printer Properties** link
- Under **Adobe PDF Settings** tab, click on **Edit** button
- Click on **Images** folder under **Standard**
- Make **Downsample** and **Compression** fields under **Color Images** and **Grayscale Images** "**Off**". And in **Monochrome Image**s field make only Downsample "Off'
- Then click on **OK** and given name of the setting in **File name** tab and click on **save**
- Then again Under **Adobe PDF Settings** tab, click on **Edit** button
- Then click on **Color** folder
- Choose **Leave Color Unchanged** option under **Color Management Policies** tab then click on **OK**
- Lastly click on **OK** in **Adobe PDF Settings** tab
- Click **Save As**
- Under **Save as type**, click the arrow next to **PDF (*.pdf)**
- Click **Save**

In Word 2003 the PDF can be created by using “Convert to Adobe PDF” symbol in tool bar or the required paper size can be adjusted in the Adobe PDF settings given in the Properties tab on the Print option. Please follow the above steps to avoid decrease in resolution and size of the figure images.

5. Reference style used in Procedia Computer Science master template:

Title	**Reference style**
PROCS	3a Embellished Vancouver