BEST PRACTICES FOR THE RISK BASED APPROACH ASSESSMENT OF THE ANTI-MONEY LAUNDERING PROGRAM WITHIN A FINANCIAL INSTITUTION

Codescu Ioana Ana-Maria*

Niculae Titulescu University, Bucharest, Romania
Commerzbank AG, Frankfurt am Main, Germany

Abstract

The Anti-Money Laundering („AML") internal controls of financial institutions are no longer implemented to satisfy the supervision authorities, but precisely to prevent risks from materializing, risks which are much higher than just a fine, such as legal, reputational or substantial financial risks. Thus, we are welcoming institutional changes on the mentality and organizational culture, with the purpose of preventing the use of the financial institutions as means for money laundering, terrorist financing or other fraud schemes.

This paper will firstly approach the „need" evolution with respect to AML measures, continuing by detailing the trends for assessing these measures.

Basically, we would like to highlight that the Compliance function, especially from the AML point of view, should represent a business actual support and not an encumbrance. In this way, compliance and business should go in the same direction, which is business development in a safe and legal environment.

Key words: anti-money laundering, counter terrorist financing, risk assessment, risk exposure, compliance, financial institutions, best practices.

JEL Classification: B41, C80, G21, G32

* Corresponding author, **Codescu Ioana Ana Maria** – anacodescu@yahoo.com
The author is employed as Head of Trade Finance AML Monitoring Group within Commerzbank AG. The opinions and analyses presented in this paper are solely owned by the author and do not have to be interpreted as owned by Commerzbank AG.

Introduction

The need for protection against financial crime within a financial institution has become a more and more complex subject, in line with the complexity of the financial crime modalities by using financial services and products.

In this respect, some of the biggest international financial institutions have been involved in big scale scandals, as they were used as vehicles for laundering illicit proceeds from crimes such as tax evasion, arms dealing, human trafficking, drug trafficking and many others alike (e.g. Deutsche Bank's involvement in the dirty money transfer from Russia to UK through capital market; Commerzbank's involvement in the famous "Panama Papers" scandal, by offering a full set of financial services and products to shell companies in Luxembourg; deficient know your customer controls of HSBC, which led to improper application of the international sanctions and so on).

The main idea of this paper refers to the fact that applying minimal standards (in accordance with the legal requirements) does not mean smaller costs. A financial institution must follow those standards which secure both the clients and the business partners. More than that, a medium-to-long term should be considered when calculating the costs. In this way, the implementation costs of complex and sophisticated compliance programs would be indeed much more increased, but only to ensure lower or even insignificant later-on maintenance costs, considering that these programs would support business lines development and expansion.

Nevertheless, in order to reach such an objective, the institutions should adapt to a different way of working, being oriented towards risk management. This means that the institution should be well informed on its own residual risk level before taking a risk based approach decision.

We will follow the line of argumentation while comparing the latest trends and best practices in this respect. But, before going forward, one should clearly understand the concept of best practices. Basically, what are best practices? They are the lessons learned by the industry from facing risks which were though improbable to materialize. Why are these best practices so important? Because a proactive approach is much better than a remediation approach, which can be much more costly. One would rather learn from other's mistakes than investing significant resources in fixing own mistakes. In the same time, one should take into account that the best practices are not only lessons to be learned, but are also benchmarks for the supervision authorities.

This paper will consider the author's practical expertise from being a compliance officer and also from working in the consultancy industry, specialized on anti-money laundering, counter terrorist financing and international sanctions.

Current needs vs. "checklist" practices

The "checklist" practices for AML internal controls implementation were intensely used in the financial sector, as the supervision authorities controls were focusing on their existence and not on their efficiency. Basically, the controls were checking whether the internal policies and procedures are in line with the national regulations (concept known as "paper based policies"). Thus, the Compliance programs should have been the same for all institutions from a particular financial sector, regardless of the business volume or the diversity of the financial products or client portfolio. Now and then, you could have received a fine for an unreported suspicious transaction. There was insufficient focus on verifying any systematic deficiencies, on checking whether a particular business line can significantly expose to risks the entire business (as the risk is contagious, it can extent to business partners also) or whether the Money Laundering Reporting Officer ("MLRO") is independent or has sufficient expertise as to report to Senior Management not only risk indicators, but the actual risk exposure (together with solutions). This was happening as these we not explicit requirements.

In May 2015, the 4th EU AML Directive ("the Directive") highlighted the need of a risk based approach in AML and not applying the same internal controls requirements among all financial institutions, regardless of their business volume or sector. It is mentioned in the Directive's Preamble that „*The risk of money laundering and terrorist financing is not the same in every case. Accordingly, a holistic, risk based approach should be used. The risk-based approach is not an unduly permissive option for Member States and obliged entities. It involves the use of evidence-based decision-making in order to target the risks of money laundering and terrorist financing facing the Union and those operating within it more effectively.*"

The Directive also recommends the financial institutions to diversify their portfolios, as long they can manage the respective risks: „*At the same time, the objectives of protecting society from crime and protecting the stability and integrity of the Union's financial system should be balanced against the need to create a regulatory environment that allows companies to grow their businesses without incurring disproportionate compliance costs*".

Considering this context and also the fact that the global fines for AML / CTF[1] / international sanctions breaches amountes up to 26 bil. Euro in the past 10 years[2], the financial institutions began customizing their AML Programs by following the internal controls standards and applying a risk based approach and not the „one-for-all" requirements. Basically, the resources allocation was made based on risk exposure, focusing more on significant risks and less on low risks.

[1] Abbreviation for Counter Terrorist Fianancing
[2] See https://www.fenergo.com/press-releases/global-financial-institutions-fined-$26-billion-for-aml-kyc.html

Right after the issuance of the Directive, its provisions were enforced by 2 guidelines which were released by the Joint European Supervision Authorities, the European Banking Authority, the European Securities and Markets Authority and the European Insurance and Occupational Pensions Authority: The Risk Factors Guidelines and the Risk/Based Supervision Guidelines – referring to using the risk based approach on both operational and supervision level. Thus, both financial institutions and supervisory authorities received elaborate guiding on how to apply the risk based approach. By customizing the AML Programs in this line, the "checklist" approach is no longer applicable.

As such, the "checklist" practice is replaced by identifying the risks and analysing the exposure and by modelling internal controls programs which effectively and efficiently manage the identified risks. Unfortunately, on the other hand, this terminology started being misused by taking "risk based approach decisions", without a proper risk assessment. This can lead to harsher consequences than applying minimum standards to a uniform extent. This is caused by the fact that the kind of decisions are not only taken on an insufficient information basis, but also on an erroneous one.

Externalizing the assessment activities

Some of the financial institutions choose to externalize the evaluation of the AML Program to consultancy companies. In this way, for the paid fee, the institution benefits from an objective opinion on the AML Program's current status and enhancement possibilities. Additionally, considering the complexity of this activity, the institution can normally continue its business activity, without allocating human resources for these activities.

However, before requesting for an offer, the institution should know its need very well, in order to properly request the consultancy services. Moreover, the institution needs also to check the professional competences of each consultant which is involved in the activities when selecting the consultancy company to work with. The company selection should be made based on practical experience in the required work stream and in that particular financial sector the institution is performing the business. Otherwise, the quality of the deliverable will not meet the expectations, the fees will be paid and the need will not be completely satisfied.

From the variety of services offered by consultancy companies, the ones which are most relevant for the present article are the Gap Analysis, the AML/CTF Risk Assessment and the Compliance Review.

The complete AML Program evaluation consists of all three above-mentioned exercises. The institution may choose to externalize one or more of these activities, or may choose to perform them on its own. Nevertheless, in case of externalising, the used methodology should be sufficient and not "negotiated" as per the paid fee.

These remarks are necessary, as there were various cases in which considerable budgets were allocated to this type of projects, however the results were unsatisfactory, affecting both the institution's interests and the consultancy company's reputation. The previous section of the article was related to "need". This needs to be very clear, for both the one who requests the services and the one offering the services. Many times, the requester does not exactly know what to ask for and the provider only assumes what is requested.

Furthermore, the requester's expectations should be in accordance with the presented offer. As such, each offer contains a short summary of the professional experience of each person who will be involved in the project. Using unexperienced persons in such projects are red flags for the deliverable's quality. In order to prevent this, the institution should take measures for knowing the consultants, similar to the know your employee measures.

The risk assessment

The assessment of money laundering and terrorist financing risks at the institutional level does not only relates to achieving the necessary conditions of the AML Program, but represents the basis of the business decision making processes. The risk assessment is undertaken in several stages and it is a continuous exercise, meaning that it ends when beginning a new one. The results must be completely and transparently reported to Senior Management, in order to set the business strategy.

The risk assessment and the business strategy of a financial institution are two interdependent elements. It is very important to note that a risky business strategy does not refers to incompliance or illegal activities, nevertheless the internal controls framework should be adequately implemented, as to efficiently manage the risks of the business activities.

As above mentioned, the risk assessment is a dynamic exercise. It starts from the criteria which were established by the best practices and international standards, which are modelled on the business risk profile of the institution, adding or removing risk indicators, as required. The assessment methodology must be adapted to the AML activity and should follow at least the following stages:

a) *Risk identification and development of the Risk Register,* which can be performed in different ways, however, in case the institution is performing this process for the first time, this stage should at least consist of documentation review, data collection through questionnaires and interviews of the key personnel in the assessed activity and review of historical data.

The process flow is a recommended and important instrument in the risk identification process, as it graphically correlates the processes within a specific activity for obtaining a better understanding of that particular activity (see *Fig. 1. Process Flow Example*[3]).

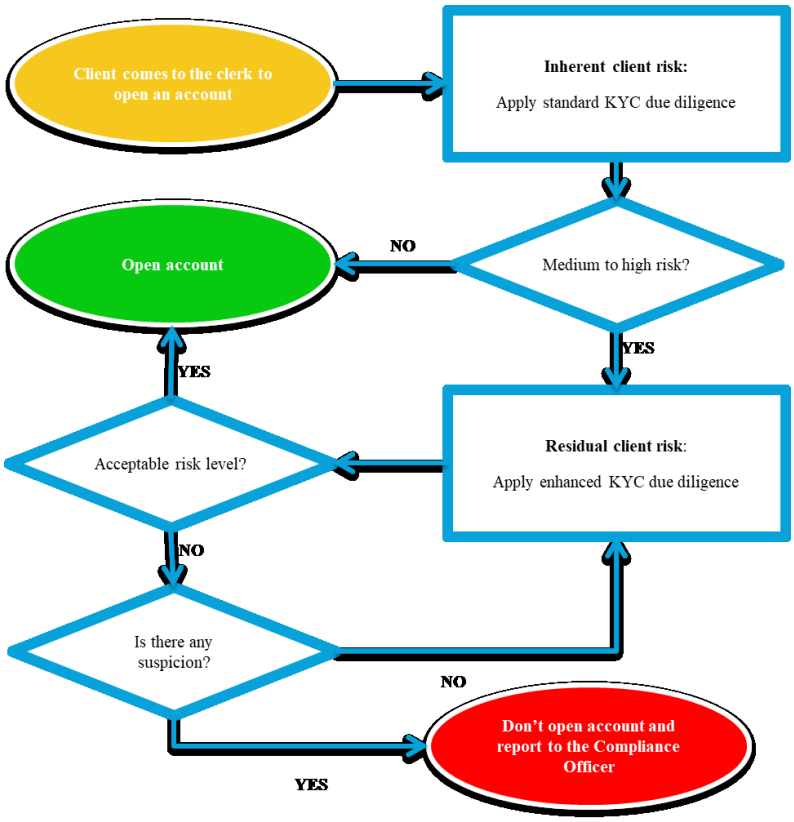

Fig. 1. Process Flow Example

The process flow must of course be designed in a complex manner, as to contain all processes which relate to a specific activity. This instrument is very useful in risk identification, but also for the identification of the existent internal controls.

[3] Graphic from own source

Besides using the process flow in the risk assessment, it can also be presented in the training sessions for the institution's personnel, considering the fact that the graphical representation has a bigger impact in acknowledging the information.

Furthermore, the assessor will consider all identified risks when drafting the Risk Register. The risks will be split into categories of main risks and secondary risks (entailed by applying risk response measures). The Register will be permanently updated and will contain information on the entire risk assessment process (a.e. each risk will contain information on the impact / probability score, the risk response measure, how will it be monitored, etc.). In usual practice, the Risk Register is the starting point of any re-evaluation and it contains the historical data showing the risk behaviour since identification (a.e. risk score fluctuation).

b) Drafting the risk assessment matrix and assessing the risks relate to the following stage in the risk assessment.

The matrix represents the tool which will be used by the assessor to calculate the risk level, based on impact and probability of materializing. Thus, the key personnel will be involved again for calculating the level of each identified risk. The assessment will consider the inherent risk (before applying the controls), the existing controls and the residual risk (after applying the controls).

When assessing a risk, the first thing to do is to design the matrixes for calculating the impact (the consequence) and the probability for materializing. As such, one can use qualitative, semi-qualitative or quantitative methods. Considering the fact that the money laundering / terrorist financing ("ML/TF") risks (client risk, transactional risk, product risk and geographical risk) cannot be always determined using similar assessment methods (e.g. geographic risk vs. product risk), the institution can choose a qualitative approach, by using charts as matrixes for calculating the impact and probability.

Moreover, in order to determine the residual risk level, the assessor will analyse the efficiency level of the existing internal controls, which were implemented with the purpose of managing the inherent risk. The analysis will consider documentation review, interviews, process flows and sample testing. After determining the efficiency level and in order to determine the residual risk level, the assessor must use the same method which was used for calculating the inherent risk.

Using a qualitative method for risk assessment has its advantages, but also its disadvantages. For example, if the assessment is not performed by a compliance and risk management experienced expert, the results may be biased by subjective factors or by error. The internal controls testing process should be thoroughly performed, in order to ensure accuracy of the efficiency level. On the other hand, the graphical representation can be very useful when determining the institution's risk appetite and risk response measures.

All results will be recorded in the Risk Register.

c) *Establishing the risk response measures* represents the strategical part of the risk assessment exercise, as it refers to a decision making process. In this respect,

considering the residual risk level, the assessor will propose measures which should be applied, according to entailed costs and the institution's risk appetite and tolerance. The risk appetite is the institution's attitude towards risk and the risk tolerance is the maximum exposure level the institution can handle (except for those situations which are approved and undertaken by Senior Management). The risk appetite level will always be under the tolerance level.

In order to determine these two criteria, the assessor must understand the business strategy of the institution. Thus, low resources can be allocated when the business strategy does not entail significant risks (Risk Adverse Strategy) or increased investments can made for implementing adequate internal controls if the business activity entails high risks (Risk Seeker Strategy). The risk assessment should be performed as to indicate the real risk level, based on which the risk response measures will be designed. The business strategy can be determined using a graphical representation of the final result of the risk assessment, which includes the risk response measures and the required resources for risk management. (See *Fig.2. Risk Appetite*[4]).

Fig. 2. Risk Appetite

In order to establish the risk response measures, the institution may choose one of the four risk management strategies:

- **Risk acceptance** – when the risk level is below the risk appetite;
- **Re-allocation of resources** – when the internal controls level is disproportionate towards the inherent risk level;
- **Risk mitigation** – by implementing new internal controls or adjusting the existing ones, in order to increase their efficiency level;

[4] Graphic from own source

- **Risk avoidance** – by eliminating the risk generating business activity.

By applying the risk response measures, the existing residual risk level is differentiated from the planned residual risk level. The existing residual risks are those which were accepted by the institution as per their acceptable level. In case risk response measures for risk mitigation or for re-allocation of resources are applied, then the resulted residual risk levels are the planned ones. That means that in the moment of performing the assessment, the existing residual risk level is still not in line with the institution's risk appetite or business strategy, but in a due time period, the risk response measure will take effect and the planned risk level will become the existing one.

The risk response measures will be prioritized according to the risk level – the main risks to approach are the highest ones. As above mentioned, risks below the appetite threshold are accepted risks. Practically, the existing internal controls are sufficient to protect the institution.

Furthermore, the assessment will consider the costs related to the implementation of these measures. As such, in order to have a risk based approach, the assessor needs to perform a cost-benefit analysis for each of the risk response measures.

The controls which let the residual risk levels below the appetite threshold do not require adjustment. However, in order to achieve a balanced cost-benefit approach, the resources which were allocated for very strong controls to low risks can be re-allocated to risks with higher impact or probability levels (see *Fig. 3. – Establishing the risk response measures*[5]).

[5] Graphic from own source

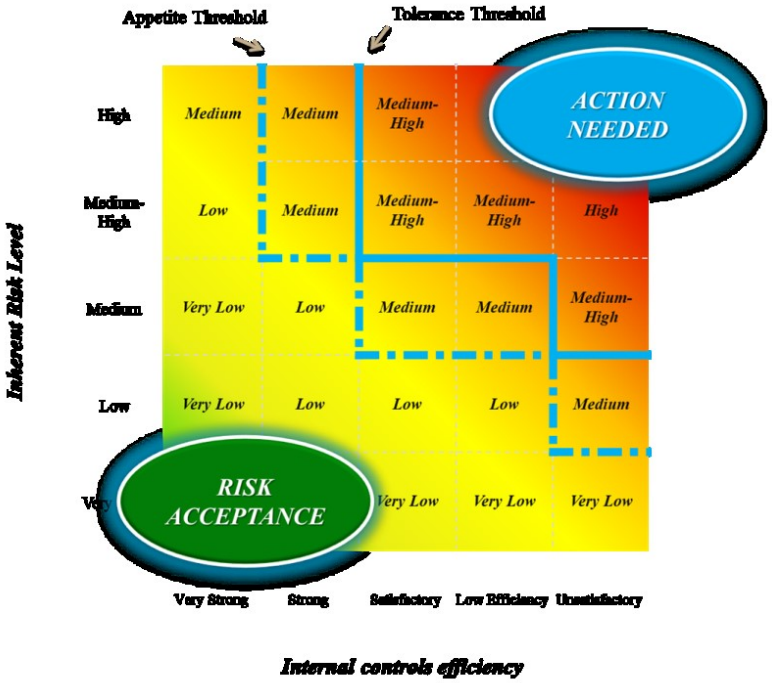

Fig. 3. Establishing the risk response measures

If the risk appetite threshold is exceeded, action is required, either by adjusting the internal controls or by implementing new ones. The purpose of the risk mitigation strategy is to establish sufficient internal controls in order to bring the residual risk level below the risk appetite threshold.

Moreover, the institution may choose a risk avoidance strategy (known as "de-risking"[6]), when the cost of risk materialization or the cost of the internal controls is exceeding the profit of the activity. For example, several international banks have exited the correspondent business relationships with other financial institutions registered in high risk countries, such as Ethiopia[7], in order to ensure no unacceptable consequences, such as

[6] The de-risking strategies are those of total avoidance of the risk, by terminating the risk generating business activities (e.g. terminating all business relationships with Iran, due to the strict sanctions which were issued by USA, through OFAC, The Office of Foreign Assets Control)
[7] Designated as high risk jurisdiction by the Financial Action Task Force

considerable fines, losing the license for specific financial products or by taking over reputational damage by association.

d) *Drafting the Monitoring Plan* ends the risk assessment process. Taking into account that the risk level has a dynamic feature, it must be periodically monitored. Additionally, the effect of the risk response measures must also be monitored, in order to ensure that the planned residual risk level will become, in a determined period of time, the real residual risk level. Basically, the intention is for the planned residual level to coincide with the existent residual level in the next risk assessment exercise.

Only after performing the full risk assessment, the institution can determine its risk based approach. It needs a thorough and meticulous analysis for the institution to focus on those risks which exceed the risk appetite threshold and to re-allocate the invested resources for control measures which are inadequate to the actual risk level.

We draw attention on the fact that the institution needs to have an accurate information basis regarding its own risks before using the "risk based approach" phrase. To support this statement, we have an example of an international bank which did not consider an informed risk based approach: the involvement of Danske Bank in the famous Russian Laundromat scandal. What happened? The bank was used for channelling 1.2 bil USD, dirty money, from Russia to other European states, through Latvia, Estonia and Denmark. When the scandal started, many of the international banks exited the correspondent relationships with this bank and the incident drew the attention of all supervisory authorities. As such, the bank paid a 2 mil. EUR fine to the Danish authorities and the Estonian branch is still under investigation. Moreover, from the moment the scandal commenced, the bank lost 22% of its market share. What went wrong? The funds were transferred through shell companies from Estonia, Latvia and Denmark, going to the UK. These shell companies were not properly identified when opening the accounts. It was thought that a funds transfer within the EU does not pose significant transactional risks, as the EU countries have a low geographical risk. The monitoring systems of the bank were inadequate, having simple and insufficient suspicion scenarios, considering the fact that the typologies were not detected. This is a very good example for the damage caused by a poor risk assessment.

The evaluation process of the AML Program

A proper assessment of the money laundering and terrorist financing risks is absolutely required for evaluating the efficiency of the implemented AML Program[8]. As above

[8] To be mentioned that the AML Program does not refer only to AML/CTF, but also to the international sanctions, thus the presented model considers this aspect too.

mentioned, knowing the risk exposure determined the risk based approach and how the AML Program must be designed.

The evaluation process of the Program contains two distinct components, the gap analysis of the policies and procedures and the compliance review of the processes (the AML internal controls). The results of these two exercises will determine the efficiency level of the anti-money laundering and counter terrorist financing prudential measures taken by the financial institution. Without going through a full description of the processes, we mention some key points that should be considered by an assessor while performing these exercises, which are drawn from best practice and industry challenges.

The Gap Analysis is the first recommended step for evaluating the AML Program, as it is an exercise in which the national and international requirements are compared against the institution's policies and procedures. The comparison detects any discrepancies between the AML/CTF/SAN[9] prudential requirements and the internal controls which were implemented within the institution in this respect.

This type of exercise does not include testing the internal controls, but only the review of the policies and procedures. Basically, the exercise does not focus on the controls' efficiency, but on their existence. This process will not give an assurance that the institution is protected from risks.

Anyhow, this analysis is just a starting point of the evaluation of the AML Program and it is very important that it considers not only the regulations and the legislation in force, but also the international standards and best practices.

The Compliance Review is the second component of the evaluation process of the AML Program efficiency, which is based on the two above mentioned activities, the Gap Analysis and the Risk Assessment. The Compliance Review will be undertaken as to approach all AML/CTF/SAN aspects and measures, which will all be verified, either through documentation review[10], process testing[11] or interviews and questionnaires[12].

With respect to the testing process, it will take into account a sufficient sample to obtain an appropriate result. The sampling will also be made according to the risk level, by allocating a bigger sample for high risk processes – for example, when verifying adequacy of the

[9] Abbreviation from International Sanctions

[10] e.g. the verification of the Senior Management reporting process will be performed by reviewing the presented risk reports

[11] e.g. the know you cutomer measures will be verified by sample testing of the client information

[12] e.g. in case the institution uses a monitoring system which is provided and supported by an external specialized company, the verification will not only consist of sample testing of the transactions, but also of questionnaires which will be sent to the external provider, in order to obtain an understnading on how and how frequently is the system audited, on any risk assessment performed on the system and what was the result, on whether there is a contingency plan in case of malfunctioning, etc.

know your customer ("KYC") measures, the testing will focus on the customer information – from the entire customer population, the testing will focus on those which entail higher risks, such as non-residents, Politically Exposed Persons, financial institution customers, etc. The sampling process will start from the entire population, on which specific selection criteria will be applied considering qualitative and quantitative elements, determining the sample for testing.

Before starting the actual review, the assessor will take into account the previous verification reports, such as the ones issued by internal and external audit, by the supervisory authorities, etc. In this way, the assessor will obtain an understanding on the deficiencies which were previously detected and will verify the remediation plans and their implementation.

The Compliance Review must follow the legal provisions which are applicable for the institution, but also consider how these provisions were approached, in accordance with the institution's risk profile. The checklist practice must be avoided, especially when the review is externalized.

For example, when verifying the *status and the role of the MLRO,* the assessor should verify whether the function is supported by Senior Management and has sufficient allocated resources to undertake its activities.

Furthermore, the MLRO needs to poses the necessary knowledge for such a position. The institution must ensure itself on this fact either by employing a highly specialized person, or by ensuring specialized training in this respect. With respect to access to information, the evaluation will check whether any restriction was detected, whether the MLRO requested lifting it and most importantly whether the MLRO appropriately uses the financial information (e.g. all transaction types are covered by the monitoring activity, all financial products and services are assessed from an AML/CTF/SAN point of view, etc.). Access to information is indeed a prerogative of the MLRO, but it's his/her responsibility whether the entire business activity of the institution is covered by the AML Program.

As mentioned, this position required advanced knowledge skills, as the money laundering phenomenon must be understood from both legal and economic points of view, in order to take the necessary measures for risk management, regardless of allocated budget or resources. I encountered in my practice small size banks with efficient AML measures and large banks with considerable allocated budgets which were using checklist practices. For example, in an international bank the AML responsibilities were so complexly granulated for the purpose of covering all risks and business activities that no one was taking any responsibility on incidents which were not in full in their area of responsibility. In another bank, excessive amounts were spent on externalizing a targeted client risk assessment on correspondent banking relationships. The result? A third of the correspondent business relationships were exited due to unacceptable risk level. It was later on proven that the risk level was exaggerated in an unjustified way, due to unspecialized persons involved in the project and to inadequate supervision of the project. On the other hand, another national bank, with a low business volume, achieved to implement a very efficient AML Program, due to a high awareness on the risk level and to allocating the resources on its risk based

approach: the monitoring systems and the efficiency of the suspicious scenarios were annually verified and adjusted accordingly, and so were the customer risk classification criteria. Moreover, all employees were periodically trained and tested on their AML awareness. Based on held interviews, the AML awareness at the bank's level was very high.

With respect to *Senior Management Reporting*, the MLRO must not only report risks or incidents, but also multiple proposed solutions. The verbally communicated issues cannot be considered by an auditor or a supervisory authority as actually communicated. Moreover, the reporting of an issue is made based on an analysis, an assessment, and an evaluation. When one would request action from the Senior Management, the request should contain sufficient information on the triggers for action, the institution's exposure and what are the proposed solutions.

Basically, the taken decisions and the implemented internal controls must be in accordance with the determined risk level, which was assessed through effective testing and thorough analyses, not with hypothesis or unrealistic estimations.

When checking the *KYC Process*, the evaluation must consider that it cannot be covered by manual controls, which are based on the user's rationale. As such, the customer risk assessment must be automatically performed, by a system. This system needs to be periodically assessed, not only concerning the used methodology, but also considering its performance and functioning. Thus, the risk classification parameters must be verified in order to check whether they contain all risk criteria and indicators and also to check whether the classification script is complete and functional.

We continue by mentioning another key aspect for the evaluation, related to the *functionality of the IT monitoring* systems. The Compliance Review requires the system to be checked similarly to an IT audit. Thus, the monitoring parameters must be checked, in order to determine whether they are sufficient and adequate for alerting transactions with risk indicators. Moreover, the transactional typologies or the suspicious scenarios should consider the historical data (a.e. historical suspicions). Least but not last, the assessor will check whether there are any periodical analyses being made on the efficiency of the typologies or scenarios, based on the review of the false positives ratio. Similarly, the customer screening process will also be subject to review in order to determine whether the matching script using the black lists has an adequate matching percentage and whether it is functional.

Furthermore, it must be ensured that the employees' transactions are also subject to monitoring for suspicious activities. In case of detecting inconsistencies, an investigation is required. In this case, the assessor will check whether the investigation procedures, the conclusions and the taken measures were not biased.

Another worth mentioning particularity in the Compliance Review process is the efficiency of the *Training Program*. The assessor must verify whether the AML/CTF/SAN training covers all employees, is adapted to need and has an adequate frequency.

Moreover, the assessor should consider that the internal auditors require specialized and thorough training, in order to properly apply their knowledge skills when performing an AML audit mission.

The Training Program is extremely important and the assessor must ensure that the entire personnel is aware of this. For example, in the international banking practice, besides the annual online training session for all employees, the information and the identified typologies are also communicated on a monthly basis through conference calls with all employees from back office or having direct contact with the customers. These conferences are organized locally, but also at the group's level. Periodically, these conferences are actually held by the CCO[13], so that the bank's personnel is aware on the bank's position towards the performance of the AML Program (a.e. the Tone from the top).

Conclusion

Replacing the checklist practices with the risk based approach indeed entails more effort from the financial institutions. On the other hand, it ensures an actual support for the business activity and does not suffocate it, as long as the risks are efficiently managed.

But it is very important to know that an efficient risk management encompasses high seriousness. A superficial risk assessment may be significantly damaging on business. The institution must be aware on what are the key points for focusing the internal controls and must de-stress the prudential measures in those areas where the risks are low.

The institutional mentality must also change, so that compliance will no longer be seen as a business enemy, but as a business partner through proper cooperation.

References

[1] AXELOS, 2010, *Management of Risk: Guidance for Practitioners (Office of Government Commerce)*, London, TSO (The Stationery Office)

[2] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission

[13] Chief Compliance Officer

Directive 2006/70/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=EN

[3] European Supervisory Authorities, *The Risk Factors Guidelines*, https://esas-joint-committee.europa.eu/Publications/Guidelines/Guidelines%20on%20Risk%20Factors_EN_04-01-2018.pdf

[4] European Supervisory Authorities, 2018, *The Risk-Based Supervision Guidelines*, https://esas-joint-committee.europa.eu/Publications/Guidelines/Joint%20Guidelines%20on%20risk-based%20supervision_EN%20%28ESAs%202016%2072%29.pdf