transcendent group GOVERNANCE RISK COMPLIANCE

AML/CTF risk assessment – core principles and future demands

By Nicolas Strömbäck

October 2020

Transcendent Group
www.transcendentgroup.com

Introduction

I have spent the better part of the past three years at the Swedish FSA reviewing AML/CTF risk assessments for various types of financial companies such as credit institutions, payment service providers and mortgage credit institutions. During this period I have had the opportunity to develop an understanding of where companies fail to complete a proper risk assessment and most often miss the core of what an AML/CTF risk assessment should be. In its recent Draft Guidelines on ML/TF risks (the DG)[1] the EBA has addressed a few such issues with risk assessment and suggested new measures to further support the development of a common understanding by firms and competent authorities of what a risk-based approach in AML/CTF entails and how firms should apply it. In this article I will look at two such common issues in light of the DG.

The purpose of this article is to highlight the importance of a *risk-based approach* to AML/CTF work within any firm, which should be part of the firms overall risk management framework. A proper risk-based approach should address relevant ML/TF risks in the business and ensure that preventive measures are commensurate to the risks identified. This will allow the firm to effectively direct resources in line with priorities and give the greatest risks the highest attention. A risk-based approach should be designed to allow the firm to establish relationships with potential customers, while effectively managing potential ML/CTF risks.[2]

A risk assessment must be "up-to-date"

During my time at the FSA most risk assessments I reviewed where inadequate or disproportionate for the business at hand. This issue seem to occur at other competent authorities as well.[3] A good risk assessment is the basis of the risk-based approach and should be proportionate to the nature and size of the firm's business. According to art 8.2 AMLD4 the risk assessment shall be *documented and kept up-to-date*. This is the first common issue many institutions fail to complete in a proper manner.

The thought of keeping a documented risk assessment up-to-date might be a no brainer for many compliance professionals but there is often a lack of understanding what the term *up-to-date* entails. It is commonplace that a financial firm in their authorization process completes the risk assessment at a "good enough"-level to be authorized and then forgets about the risk assessment in part or entirely, effectively making the risk assessment a *desktop product*, not necessarily designed to cope with external and internal incident and evolving risk-monitoring to identify emerging risk in terms of ML/TF. Such an approach is doomed to fail in the long run and may be subject to measures from the FSA.

---

[1] JC 2019 87 CP.
[2] FATF - Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing - High Level Principles and Procedures, June 2007, p. 2.
[3] JC 2019 87 CP p. 7. In ref. to ESAs Joint Opinions on ML/TF risks, JC/2017/07 and JC2019 59.

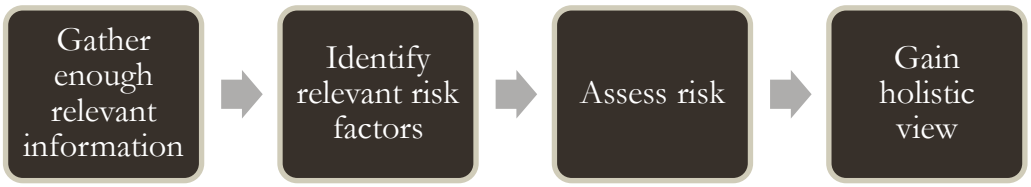
There has previously been little clarification as to what the term up-to-date means. In the DG the EBA offers a new description:

"1.4. Firms should record and document their business-wide risk assessment, as well as any changes made to this risk assessment in a way that makes it possible for the firm, and for competent authorities, to understand how it was conducted, and why it was conducted in a particular way."

This will mean that risk assessments will need more transparency, e.g. with a detailed revision history where all changes made are included. The use of a detailed revision history for risk assessment documents isn't commonplace today but is recommended going forth to stay compliant.

Then, you might ask, what is the best way to keep a risk assessment up-to-date?

The first step is to ensure that the firm has an adequate risk assessment to begin with. If the firm hasn't kept its assessment up-to-date chances are it needs revision. This should be completed using the following steps:



Gather enough relevant information is the most important part of the risk assessment and something the FSA will remark on if it isn't up to par. Typically this means taking into consideration internal information (from ongoing business relationships etc.) and external information from governing authorities (national and international risk assessments, FATF recommendations, EBA guidelines etc.). It isn't enough to just refer to such information in the risk assessment. There must be a record of which information the firm has considered and why, in sufficient detail. This is especially important for high risk-operations where such information is deemed critical.

Identify relevant risk factors is normally done when the risk assessment is first created. It is however crucial for the institution to maintain a flexible and relevant view on its risk factors, being open to changing and/or adding factors. This is closely connected to the gathering of relevant information as new information could shed light on possible risks that needs to be considered.[4]

Assess risk should be done in light of the information gathered, both internal and external. It is important for the firm to consider relevant risk factors at different levels across the spectrum and classify these into categories[5]. Such classification of risks, when done

[4] As seen in the Swedish FSA:s sanction against Swedbank AB, where the managements reluctancy to consider new information about the Baltic affiliates led to a warning and fines of 4 MSEK, FI Dnr 18-21044 och FI Dnr 19-7504, p. 2 f. and p. 25 ff.
[5] JC 2019 87 CP, Guideline 3.8-3.9.

properly, will make the continuous assessment of risks easier, and will thus give the organization a better overview of its entire risk spectrum.

Gain holistic view could be described as taking a step back, reviewing the information gathered and risks assessed to see the bigger picture. Questions to ask can be:

- Have we identified all risk factors?
- Does the result of the assessment cast new light on our operations?
- How does the assessment affect what actions we need to take?
- Is our assessment relevant in light of gathered information on customers and transactions?
- Can this assessment enable us to make good and relevant business decisions?

This is a general overview but the steps mentioned should be a good starting point for reviewing the risk assessment, making sure it is in line with the purpose of the framework, while still enabling the firm to make reasonable business decisions with respect to its customers.

The second step is to ensure that the firm has proper systems and controls in place to keep the revised risk assessment up-to-date. The DG offer new guidance on what this entails.

A firm should:

1. Have systems and controls in place to
    a) Keep its AML/CTF-risk assessment associated with its business
    b) Review ongoing relationships to stay updated
    c) Identify emerging ML/TF risks, assess these risks and, where appropriate, incorporate them into its business-wide and individual risk assessments in a timely manner
2. System and controls put in place should include (in short):
    a) Regular review of internal information to identify trends in relationships and transactions
    b) Regular review of external information from relevant sources such as financial sanctions, media reports, law enforcement reports, publications by competent authorities etc.
    c) Engagement with other industry representatives and competent authorities

This second step is a welcome addition to the framework as it delivers a hands-on approach that firms can use as a guide in its risk-based approach to AML/CTF work. When applied properly it should make the risk-based approach more effective in assisting the firm in preventing ML/TF and be able to exercise reasonable business judgement with respect to its customers.

AML and CTF are different activities

The second common issue is that firms don't regard ML and TF as separate activities that need different risk assessments, but instead consolidate them as the same activity, thinking the risks are equal. This results in an inadequate risk assessment that doesn't consider actual risks and effectively will make suggested measures ineffective or non-relevant.

The most common approach is that firms base their risk assessment on risks adherent to ML and align TF with these risks. In some instances there are of course overlapping risks between ML and TF but they still need to be assessed in different ways as the measures required most likely differ. It is important that the firm – in its risk-based approach – understands the difference between ML and TF risks, document these risks in a distinctive manner, making them available for supervising authorities, and then establish distinct separate measures to prevent or minimize these risks.

This separation of ML and TF risks isn't explicitly stated in the DG but can be derived from Guideline 2 where they are clearly treated as separate activities.

Conclusion

The AML/CTF regulatory framework will become more comprehensive as the scope of financial crime becomes clearer to governing bodies. The demands on firms will become more far-reaching in terms of adequate risk assessments. My guess is that it will be near impossible for any firm to be authorised or stay authorised should their AML/CTF risk assessment be flawed or not properly adapted and updated in light of the business at hand. It is therefore crucial for firms to lock in their *risk-based approach* which includes:

- understanding their business,
- understanding the framework,
- understanding, identifying and classifying their risks,
- assessing these risks,
- gaining a holistic view of the entire business, its customers and transactions and
- complete processes to keep risk assessment up-to-date.

Sanctions like the one awarded to Swedbank in Sweden and matters related to Danske Bank in Denmark and Deutsche Bank in Germany is the beginning of tougher supervision by authorities, a more comprehensive legal framework and stricter penalties. Whether this is good or bad I will refrain from commenting on, but it is certain that the compliance role will need to evolve with these changes and most likely adapt in terms of the usage of technological means to identify and assess risks.

This article is a preview of some of the content and questions that I will expound upon in a future AML/CTF-education series being held by Transcendent Group.

Nicolas Strömbäck

+46 (0) 70 234 87 10

nicolas.stromback@transcendentgroup.com