Financial crime risk assessment

Legislation in force to prevent financial crime has become more risk focused, requiring organizations to fully understand the risks their organization faces based on their business model and strategy. Companies' financial crime controls are increasingly in the crosshairs of regulators. Therefore, embedding financial crime controls in a risk management framework and developing a robust risk assessment tool around this framework has become a key priority. The following article discusses the recently published risk assessment approach[1] set out by the Wolfsberg Group and looks at possible approaches that might be considered based on EU and U.K. regulatory requirements.

Some risk assessment guidance

The Financial Conduct Authority's (FCA) guide *Financial crime: A guide for firms*, published in April 2015,[2] underlines that a thorough understanding of a firm's financial crime risks is key if a firm is to apply proportionate and effective systems and controls. Likewise, the Wolfsberg Group noted in a recent publication titled *Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions, and Bribery and Corruption* that a risk assessment framework is the basis from which organizations can derive risk indicators and assess their financial crime risk exposure.[3]

A risk assessment should be embedded in a risk-based approach, which relies on a risk framework. This framework should include identifiable risk metrics, thus providing the most effective levels of compliance and ability to detect, report and prevent corruption, money laundering (ML), fraud, sanctions violations, terrorist financing (TF) and tax evasion.

The FCA's publication, *Financial crime: A guide for firms*,[4] provides guidance on developing a risk assessment. It sets out the following key questions which organizations setting out to undertake a risk assessment should strive to answer:

---

1 Wolfsberg Group, http://www.wolfsberg-principles.com/

2 The Financial Conduct Authority, "Money Laundering," February 7, 2015, http://www.fca.org.uk/about/what/enforcing/money-laundering

3 Wolfsberg Group, "Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery and Corruption," 2015, http://www.wolfsberg-principles.com/pdf/home/Wolfsberg-Risk-Assessment-FAQs-2015.pdf

4 The Financial Conduct Authority, "Financial crime: A guide for firms," December 2011, https://www.fca.org.uk/static/documents/policy-statements/fsa-ps11-15.pdf

- "What are the main financial crime risks to the business?
- How does your firm seek to understand the financial crime risks it faces?
- When did the firm last update its risk assessment?
- How do you identify new or emerging financial crime risks?
- Is there evidence that risk is considered and recorded systematically, assessments are updated and sign-off is appropriate?
- Who challenges risk assessments and how? Is this process sufficiently rigorous and well-documented?
- How do procedures on the ground adapt to emerging risks?"[5]

According to the FCA, a good practice risk assessment framework is comprehensive, continuous and based on best available sources of internal and external information, and concentrates its resources on higher risks. Furthermore, it "actively considers the impact of crime on customers" and thus "considers financial crime when designing new products and services."[6]

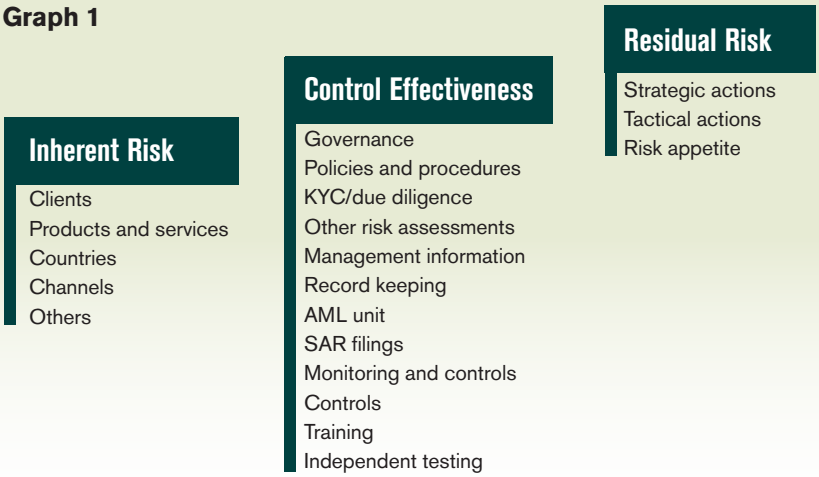
In late October 2015, a joint Committee of the three European Supervisory Authorities (EBA, EIOPA and ESMA—ESAs) launched a public consultation on two anti-money laundering and counter-terrorist financing (AML/CTF) guidelines. The consultation closes on January 22, 2016. The ESAs will hold a public hearing on the draft guidelines, which will take place at the EBA premises in London on December 15, 2015. According to the press release published by the EBA, these guidelines promote a common understanding of the risk-based approach to AML/CTF and set out how it should be applied by credit and financial institutions and competent authorities across the EU.[7] The consultation papers underline that customer due diligence (CDD) is central to the process of managing financial crime risk for both risk assessment and risk management. An upcoming article to be published in early 2016 in *ACAMS Today* will further expand upon the details of the ESA's proposed guidelines specifically in relation to CDD requirements.

Wolfsberg's approach to financial crime risk assessment

According to the Wolfsberg Group, a three-phased approach (see Graphic 1), which it terms as the "conventional/standard methodology," can be adopted in order to undertake a risk assessment.

1. Determining inherent risk—Inherent risk represents the exposure to financial crime in the absence of any control environment being applied.[8] These risks can vary from organization to organization and must be defined in a risk-based manner—a key challenge at the heart of developing an adequate risk assessment tool. Guidance on indicators and red flags is provided by regulators and organizations, such as the Wolfsberg Group.
2. Assessment of internal controls—Once the risks have been identified, internal controls (policies, procedures and other activities) need to be mapped against these risks in order to assess how effectively they offset the overall risks.[9]
3. Deriving residual risk—Once the inherent risk and the effectiveness of internal controls have been evaluated, the residual risk can be determined.[10]

Graph 1



(Source: Based on the Wolfsberg Group's FAQ on Risk Assessment)

[5] Ibid.
[6] The Financial Conduct Authority, "Financial crime: A guide for firms," December 2011, https://www.fca.org.uk/static/documents/policy-statements/fsa-ps11-15.pdf
[7] http://www.eba.europa.eu/-/eba-eiopa-and-esma-consult-on-anti-money-laundering-and-countering-the-financing-of-terrorism
[8] Wolfsberg Group, "Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery and Corruption," 2015, http://www.wolfsberg-principles.com/pdf/home/Wolfsberg-Risk-Assessment-FAQs-2015.pdf
[9] Wolfsberg Group, "Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery and Corruption," 2015, http://www.wolfsberg-principles.com/pdf/home/Wolfsberg-Risk-Assessment-FAQs-2015.pdf
[10] Wolfsberg Group, "Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery and Corruption," 2015, http://www.wolfsberg-principles.com/pdf/home/Wolfsberg-Risk-Assessment-FAQs-2015.pdf

Table 1

COUNTRY RISK

The overall reputation of a country should be factored into the risk model. For example, certain countries or jurisdictions have high levels of corruption or unstable governments. Some are known as bank secrecy and ML havens or suffer from high levels of drug production and shipping, and cartel activities. Information sources to help identify reputational risk include Transparency International's Corruption Perceptions Index and the U.S. State Department's annual International Narcotics Control Strategy Report (INCSR), which rates countries based on their ML controls and corruption.

It is important to establish a documented geography risk rating methodology that leverages internal and external information sources, including at least a review of sanctions and TF lists published by governments and international organizations such as those published by the U.S. Office of Foreign Assets Control (OFAC), the U.K. FCA, the U.N. Security Council Committee, the U.S. Financial Crimes Enforcement Network (FinCEN) and the EU.

The risk model may take into account whether a country is a member of the Financial Action Task Force (FATF) or of an FATF-style regional body, and has implemented practices in line with international standards set out by the FATF and other international organizations.

The risk model should also take into account regional risks inside a particular country, such as the cross-border areas between nations, or designated areas of high intensity financial crime or drug trafficking, such as the U.S. High Intensity Financial Crime Areas or High Intensity Drug Trafficking Areas.

PRODUCT/TRANSACTION RISK

Common product and transaction risks include the following whereby each product will in turn have its own red flags.

- Wealth management
- Trusts and foundations
- Relationship to correspondent banks
- Mobile payments
- Value transfer through virtual worlds and digital currencies
- Payable through accounts and concentration accounts
- Life insurance and annuities

Red flags for trade-based finance might include the following:

- Private banking and correspondent banking
- Payments to vendors in cash by unrelated third parties
- Payments to vendors by wire transfers from unrelated third parties
- Payments to vendors by checks, bank drafts or postal money orders from unrelated third parties
- False reporting, such as commodity misclassification, over-valuation or under-valuation
- Carousel transactions, meaning repeated importation and exportation of the same high-value commodity
- Trading in commodities that do not match the business
- Unusual shipping routes or transshipment points
- Packaging that is inconsistent with the commodity or shipping method
- Double-invoicing

CUSTOMER RISK

The following includes a list of red flags attached to customers. Beyond those listed below, any indirect risks which emerge through association or other issues which are of reputational concern and which undermine the integrity of the customer should be identified. It is useful to consult other red flag check lists included in FATF reports, the *Good Practice Guidelines on Conducting Third Party Due Diligence* (published by the World Economic Forum in 2013), or other sources like Australia's FIU, which has published some 70 red flag indicators.

- Foreign financial institutions
- Targets of financial sanctions
- Non-bank financial institutions
- Intransparent beneficial ownership
- Contradictory information
- Politically exposed persons (PEPs)
- Third-party relationships
- Offshore structures
- Shell companies or shelf companies

SECTOR RISK

Some sector risks–regarding corruption and bribery, in particular–might include the following:

- Sectors which are strongly influenced by government or state-owned entities
- Public sector procurement and government contracts
- Sectors which are not subject to regulation
- Sectors in which corrupt practices are endemic

According to the *OECD Foreign Bribery Report* (2014),[10] those sectors most exposed to corrupt practices include the following:

- Commodities sector
- Real estate
- Transport
- Information and communication
- Manufacturing business
- Health care
- Utilities
- Gas sector

Sectors particularly vulnerable to ML include the above, but in particular they include the financial services sectors and companies trading in consumer goods.

Alternative approaches to risk assessments

Based on the category guidance provided in the Annex of the Fourth EU AML/CTF Directive (see article on the Fourth EU AML/CTF Directive published in the September-November 2015 edition of *ACAMS Today*[11]), the following three-step approach—risk modeling, risk filtering and risk rating—for the development of a risk assessment framework, might be adopted.

- Risk modeling
  —Comprehensive audit of potential sources of risk
- Risk filtering
  —Identify the most relevant red flags
- Risk rating
  —Quantitative assessment of risk

The risk modeling phase involves a comprehensive audit of potential sources of risk based on compliance regulation and legislation, both national and international, as well as international best practice standards. Four categories—customer, country, product/transaction and sector—are typically those around which a risk assessment can be modeled. This model framework can be expanded to include other risk areas such as transaction risk and process risks. Some risk scoring models limit their framework to the "triad" of customer, product/service and geography.

The risk filtering phase, which is built on the risk modeling phase, focuses on identifying the most relevant compliance risk factors facing the institution, in respect to financial crime. A detailed understanding of the often, interconnected compliance risks emerges. This is the phase where the focus lies on identifying red flags. This phase is important as it helps to zone in and focus on those risks, which are of most concern to an organization. See Table 1 for a selection of risk indicators and red flags. This is not a comprehensive list, and should be complemented by continuous research and reference to emerging risks and crime trends.

The risk rating phase assesses both the seriousness of risks identified in the risk-filtering phase and the certainty of information and the reliability of sources on which the indications are based. The assessment results in the ranking of high risks, medium risks and low risks on the basis of which risk-based decisions can be made and risk mitigation strategies developed. The effectiveness of these decisions and strategies can be evaluated via a risk monitoring procedure.

Financial crime and risk management

Financial crime risk assessment is the first step in managing the risks associated with financial crime. The design of a risk assessment framework will depend on the complexity and structure of an organization, the markets and countries in which it is active as well as its client base. As set out by the Wolfsberg Group,[12] the following achievements can be derived from undertaking a risk assessment regardless of the approach taken. This is based on the assumption that the quality of the data is high and the selection of the risk indicators is effective.

- Identify gaps or opportunities for improvement in AML policies, procedures and processes
- Make informed decisions about risk appetite and implementation of control efforts, allocation of resources, technology spend
- Develop risk mitigation strategies including applicable internal controls and therefore reduce a business unit or business line's residual risk exposure

These measures can assist management in the following areas:

- Understanding how the structure of a business unit or business line's AML compliance program aligns with its risk profile
- Being made aware of the key risks, control gaps and remediation efforts
- Strategic decisions in relation to commercial exits and disposals
- Ensuring that resources and priorities are aligned with its risks

Summary

Although the Wolfsberg Group notes that risk assessments are only one element of the financial crime compliance toolbox, it is important to highlight their current relevance due to the increased regulatory focus on this area both at an enterprise-wide level as well as at the individual level of any one customer. Financial crime risk assessment is seen as the cornerstone of financial crime prevention as it is the underlying tool for identifying, quantifying, documenting, monitoring and managing financial crime risks both horizontally across the entire business, as well as vertically down to any one individual customer relationship.

Jennifer Hanley-Giersch, CAMS, managing partner, Berlin Risk Ltd., Berlin, Germany, jennifer.hanley@berlinrisk.com

[10] OECD, "Foreign Bribery Report: An Analysis of the Crime of Bribery of Foregin Public Officials," 2014, http://www.keepeek.com/Digital-Asset-Management/oecd/governance/oecd-foreign-bribery-report_9789264226616-en#page1

[11] Jennifer Hanley-Giersch, "The Fourth EU AML/CTF Directive: A Holistic Risk-Based Approach," *ACAMS Today*, September-November 2015, http://www.acamstoday.org/fourth-eu-aml-ctf-directive/

[12] Wolfsberg Group, "Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery and Corruption," 2015, http://www.wolfsberg-principles.com/pdf/home/Wolfsberg-Risk-Assessment-FAQs-2015.pdf