FINANCIAL CRIME RISK MANAGEMENT USING KEY RISK INDICATORS

Compliance professionals are no longer expected to just manage existing risks, but to anticipate arising risks that could negatively impact the reputation of the firm and imposition of regulatory sanctions, fines, or penalties. Such proactive financial crime risk management involves use of existing data, organized in meaningful patterns, which can inform the dimension and direction of risk and consequent decisions and actions. This requires a more comprehensive risk management program that includes a robust risk identification and assessment of the financial crime risk profile of the bank/unit and selection of tools and processes to effectively manage risk exposure including through the active use of Key Risk Indicators.

KEY RISK INDICATORS

Key Risk Indicators (KRIs) are metrics and/or statistics used to monitor the main drivers of exposure associated with key risks and have long been in use for other risk types such as credit, market, and operational risk management. KRIs provide early warning signals while also tracking trends over a period of time, assisting management in understanding current and changing risk exposures which may indicate need for action. For example, a large increase in the number of non-resident non-national account holders in the bank's portfolio at a particular branch may not be consistent with the bank's risk appetite.

As KRIs provide insights on exposures and accordingly direction on decisions and actions, it is important that they are designed with care. In choosing KRIs, a compliance officer should consider the potential financial crime issues that may arise, taking into consideration inherent financial crime risks in its core markets, the nature of the bank's products, clients and processes, and the impact of risk management failures in terms of regulatory and reputational consequences. By way of example, maintaining an account for a known terrorist would have far more consequences than omitting to fill a single Cash Transaction Slip. Additionally, KRIs should be associated with reasonable trigger levels and thresholds based on an entity's risk appetite and tolerance, or internal risk acceptance.

Unfortunately, there is no off-the-shelf set of KRIs for firms to deploy. It differs according to each firm's circumstances, products offered, target markets, client base, regulatory requirements and geographic scope. However, a critical success factor is to deploy various sets of metrics that complement each other providing a holistic view of risks associated with an entity's business as well as those arising from controls failing to work as intended. The following sections offer general examples of different types of KRIs.

IDENTIFYING AML / CTF / SANCTIONS RISK EXPOSURE

Regulators are increasingly looking for evidence that management takes into consideration objective measurements of risk and understanding of the entity's financial crime risk exposure when making decisions. Several regulators require formal risk as-

HIGH RISK INDICATORS - % OF:

- High Risk Accounts
- Politically Exposed Persons (PEPs)
- Customers with High Risk Nationality and/or Residency
- Non national non resident customers
- Transfers to/from countries subject to sanctions and embargo
- Accounts related to Known Tax Haven Countries
- Accounts opened on non face-to-face basis
- Trade finance transactions involving High Risk Goods, e.g. dual-use goods, oil
- Dormant accounts activated / dormant accounts with credit transactions
- Incoming transfers with missing KYC data

SPECIFIC TO CORRESPONDENT BANKING - % OF:

- FIs offering Payable Through Accounts
- FIs offering Nested Accounts
- FIs offering Numbered Accounts

sessments to be conducted on a regular basis. Yet, financial crime regulations and guidance are rarely detailed enough to provide direct, quantitative guidelines on how to define an entity's risk profile.

As a general guide, a comprehensive profile should encompass an entity's customer types, the types of products and services offered and the manner through which they are provided, as well as jurisdictions with which the entity operates or conducts business, i.e. a customer / product / channel / geography analysis. Such analysis may be conducted at each business level (e.g. retail, corporate, etc.) as well as entity or geography level (e.g. UK subsidiary). Care should be taken not to de-risk wholesale classes of customers or geographies, but rather to set controls to manage risks effectively and efficiently within the institution's internal risk appetite.

The purpose of KRIs is to generate actionable intelligence. As such, compliance officers should consider whether the risk assessment results signal need for action. By way of example, a significant number of unrated accounts may signal the need for increased AML/CTF training to front-office staff while a spike in trade finance transactions that does not result in an increase in escalated high risk transactions may warrant increased resources to manage evolving business needs.

ENSURING CRITICAL CONTROLS WORK AS INTENDED

Having identified the initial entity AML/CTF/Sanctions risk profile, it is necessary to ensure controls addressing most critical risks are working as intended. This requires defining objective KRIs in the areas where the process breaks and creates exposure to a particular risk. Identifying critical process weaknesses ensures no material risk is left unattended and provides the basis for risk-based, efficient oversight and corrective activities. Examples:

KYC/CDD

- % of Non Risk Rated Customers
- % of Accounts with KYC alerts outstanding > 30 days
- % of Accounts with incomplete CDD/KYC
- # Accounts Opening Declined by Compliance

Investigation

- % of Alerts Outstanding > 60 days
- % of System generated alerts that resulted in a SAR
- # of Customers identified as subject to regulatory enquiry
- Average time for filing a SAR

Sanctions

- # of Customer database screening alerts outstanding > 30 days
- % of Genuine hits during customer on-boarding
- % of Genuine hits during periodic customer screening
- # of Payment screening alerts generated versus total # of payments

VALIDATING EFFECTIVENESS OF AML / CTF PROGRAMS

Regulators and international standard setters are increasingly focusing on the effectiveness of AML/CTF/Sanctions programs. This is also becoming an area of concern for banks' Boards as regulators expect their active involvement in ensuring risks are appropriately identified and in overseeing the effective management of the financial crime program. More recently, the need for meaningful metrics to measure effectiveness has reached a tipping point with regulators seeking to hold board members, senior management, and compliance officers personally liable for weak AML/CTF/Sanctions programs.

The following examples of KRIs are beneficial in validating the effectiveness and efficiency of AML/CTF programs.

AML/CTF Breaches (Regulatory & Internal)	# of Compliance breaches # of repeated Compliance breaches
	# of High Risk Compliance breaches
	# of overdue issues without risk acceptance/approved extension
AML/CTF Training	% of staff who have not completed the mandatory AML/CTF training
	% of new hires who have not completed the mandatory AML/CTF training within (X) months from employment

CONCLUSION

In an increasingly complex and rapidly changing environment, compliance officers must not be complacent. They must continually seek to improve on the ability to understand evolving risks and take pre-emptive steps to manage and mitigate AML/CTF/sanctions risk exposures. Effective KRIs provide a lens on where the firm stands in terms of existing risk exposures and actionable intelligence for decisions, actions and directions. Risk assessments and KRIs should be refreshed periodically to ensure they remain relevant for the entity, as the environment is dynamic. In short, KRIs constitute a critical element for robust AML/CTF risk identification, monitoring, and mitigation, forming the bedrock for a meaningful and sustainable AML/CTF/Sanctions program.

ABOUT THE AUTHORS

MICHAEL MATOSSIAN, EVP AND CHIEF COMPLIANCE OFFICER

Joined Arab Bank plc in November 2005 as EVP and Global Head of Group Regulatory Compliance. Mr. Matossian has more than 30 years of experience in regulatory risk management, anti-money laundering, and compliance. Mr. Matossian participates on several national and international task forces addressing governance, anti-money laundering, and compliance matters and is the Founding Member and Deputy Chair of the MENA Financial Crime Compliance Group.

SHARON CRAGGS, GROUP COMPLIANCE OFFICER

Presently is the Group Compliance Officer for the Arab Banking Corporation (ABC), Bahrain. She has experience across private and public sectors, managing diverse teams across developed and emerging market jurisdictions, with expertise in multiple product lines including financial markets, corporate banking, consumer banking, wealth management, and financial crime compliance. Sharon holds the Chartered Financial Analyst (CFA) and Chartered Alternative Investment Analyst (CAIA) designations, and was appointed Distinguished Fellow of the Institute of Banking and Finance by the Singapore Minister for Finance.

MENA FCCG

The MENA Financial Crime Compliance Group (MENA FCCG) is a voluntary body that seeks to bring collective action in the fight against money laundering and terrorist finance in the region. The group comprises 12 banks representing eight MENA countries, including; Bahrain, Egypt, Jordan, Kuwait, Lebanon, Oman, Qatar, and the UAE. The Group is presided over by Wissam H. Fattouh, Secretary General for the Union of Arab Banks while Michael Matossian is the current Deputy Chair.

MENA FCCG
Making a Collective Impact