Managing compliance risk

Where are you now?

It is often said that the only constant is change; and when reflecting on the current Middle East regulatory landscape, this certainly holds true. With the tide of regulatory change expected to remain in the medium-term, can compliance officers in the region be confident that they are keeping up with the wave of change?

It's all a matter of priority

In keeping with international trends, and reflecting the ongoing emphasis of international legislation and enforcement activity, managing Compliance Risk remains a high priority for organizations across the Middle East North Africa (MENA) region. Anti-Money Laundering (AML), sanctions, fraud and Counter Terrorism Financing (CTF) continue to top the list of initiatives that businesses are taking to counter financial crime.

Interestingly though, while we have seen progress globally in the fight against bribery and corruption in recent years, the existence of Anti-Bribery and Corruption (ABC) policies continues to lag behind for organizations in the region. This lag is expected to be addressed in the short-term as Middle East economies continue to integrate with the wider global community through inward and outward investment.

Perhaps the most noteworthy concern in terms of prioritizing financial crime risk is that, despite the current global focus on cyber security issues including hacking, data losses or breaches and other information leaks, organizations across the Middle East still do not have formal cyber security initiatives in place.

While we have seen progress globally in the fight against bribery and corruption in recent years, the existence of Anti-Bribery and Corruption (ABC) policies continues to lag behind for organizations in the region

As a region known for its financial services and energy interests (both of which require a high degree of confidentiality of information) the Middle East represents an attractive target for cyber criminals. Industry research reveals increased cyber security threats in the Gulf Cooperation Council (GCC) region, which we have seen manifest in the widespread banking malware in the United Arab Emirates (UAE) and recent phishing attacks in Saudi Arabia.

With the increasing focus on cyber security by prominent experts, authorities and media houses, the apparent lack of policy on the issue is counter-intuitive but is reflective of a historical deficiency in both, the setting of clear and active local regulation, as well as in in-house efforts to combat the ever-increasing threat cyber security poses. Change is soon to set in however, as both local and international governments push the issue of cyber security to the top of their political and legislative agenda. We expect this will become an increasingly prominent concern for companies in the Middle East region, particularly given the level of reliance on technology being used to fight financial crime.

Reputation is critical

The risk of reputational damage associated with compliance failures continues to be the key driver for managing compliance risks in the Middle East. Increasingly though, businesses are having to balance regulatory compliance with furthering their business objectives. That these two points should be at the top of the corporate wish list is reflective of the ongoing transformation of organizations in many economies across the Middle East region following the global financial crisis.

A key challenge continues to exist for organizations in emerging markets: to balance meeting these two seemingly competing priorities while maintaining business integrity. Banks in the GCC, for example, have had a traditionally low customer penetration rate and are changing their focus to attract and retain customers from untapped markets. In this environment, differentiation is important, which means that reputation is vital. The possible loss of correspondent banking relationships–which limits the ability of regional financial institutions to operate in a truly global capacity–for compliance-related reasons is just one example of the potential fallout of compliance failures.

Low levels of confidence in existing compliance programs

Of big concern is that while organizations appear to have assessed the key compliance risks affecting their businesses, their ability to manage these risks using existing compliance programs is limited. In a recent survey[1] conducted by Deloitte, almost half of respondents highlighted a lack of confidence in the effectiveness of their existing financial crime programs when compared with both domestic and international regulatory requirements, while over 50 percent of those surveyed questioned the ability of their compliance policy to prevent illicit activity.

This lack of effectiveness is particularly noteworthy given that many locally established financial institutions are actively looking to expand their presence globally, either by expanding into other jurisdictions or through the acquisition of customer bases. This is in line with international trends and reflects an ever-changing regulatory environment, combined with an absence of structured and robust regulatory guidelines in certain jurisdictions.

If financial crime programs are not meeting the current regulatory needs, their ability to support ongoing strategic or operational change in a time of ongoing

regulatory uncertainty poses a key risk. The responses also point to the potential for vulnerability to the impact of financial crime. Financial crime is quite often linked to terrorist funding, so should a financial institution be so implicated, it can result in a devastating fine and tarnishing of reputation.

The above weaknesses also highlight the importance of the culture of compliance management existing within organizations. Having comprehensive written policies is meaningless as we see more and more financial institutions having to demonstrate to regulatory agencies that they have effectively embedded policies into the business.

Are organizations managing risks effectively?

Organizations continue to rely upon a combination of people, process and technology to manage compliance risks. However, against a backdrop of increasing costs and scarcity of appropriately trained resources, businesses are increasingly turning to technology as the primary means of managing compliance risk. While this highlights the need for greater efficiency at a time where budgetary pressures continue to exist, fighting financial crime requires a multi-faceted approach.

Sanctions, fraud and Anti-Bribery and Corruption (ABC) programs management depend on due diligence and technology, while AML programs mainly use customer on-boarding and profiling and due diligence to reveal risk. Combating the Financing of Terrorism (CFT) relies on suspicious transaction reporting and technology, and of course, cyber security is largely technology-based. However, as the regulatory environment has evolved over the past decade, Know Your Customer (KYC) processes have increased in their complexity and now require a more sophisticated response. Human capital and specialist skills will continue to be sought after, and the organizations that succeed will be those that are continuing to invest in recruiting and training staff.

Similarly, technology continues to be the most efficient method of managing 'business as usual' processes such as transaction monitoring, while the use of regulatory intelligence is also becoming more prominent as firms seek to balance the cost of compliance with the need to remain vigilant on combatting financial crime. While historically it has tended to be used as a reactive measure, as with most compliance activity, the true benefit of this work comes with undertaking it proactively.

Although the future of financial crime management appears to be in the use of technology, businesses in the Middle East region need to ensure they are not overly reliant on it

Although the future of financial crime management appears to be in the use of technology, businesses in the Middle East region need to ensure they are not overly reliant on it. We expect that effective compliance programs will continue to demand a balance of technology with human intervention to ultimately serve to manage the risks associated with operating in the region.

Managing financial crime risk remains one of the most important challenge organizations in the Middle East face going forward. The need for compliance officers to anticipate regulatory change, think smarter about managing the associated risks and maintain the visibility of regulatory efforts on the C-suite agenda has never been greater. Similarly, regulators need to support organizations by providing robust regulatory support for managing the fight against financial crime. Only then will we see the tide of regulatory change turn.

by **Mandy Green**, Director, Forensic Services, Deloitte Corporate Finance Limited (regulated by the Dubai Financial Services Authority)

Endnotes

1. In Q3, 2014, together with Thomson Reuters, Deloitte launched a joint survey of financial crime programs in the Middle East. www.deloitte.com/financialcrimesinmena2015