Corporate compliance: stepping outside the comfort zone

While financial institutions have traditionally been the target of regulatory focus, corporates now face growing pressure to comply with sanctions and AML requirements.

Corporates face growing pressure to implement effective financial crime controls to mitigate regulatory and reputational risks which could otherwise damage their ability to conduct core business activities. To do this, corporates are increasingly adopting the types of compliance solutions which have traditionally been used by banks. In this challenging environment, developments such as the US Department of Justice's recently published guidelines on corporate compliance can provide a valuable insight into regulators' expectations.

For corporates around the world, compliance with financial crime regulations is a greater concern than ever before. Increasingly, corporations are expected to take a proactive approach in order to comply with sanctions and anti-money laundering (AML) regulations.

The importance of putting suitable controls in place has been underlined by the growing number of corporates that have been charged with errors or mistakes in their financial crime compliance processes. Actions in recent years include PayPal's $7.7 million fine in 2015 by the US government for failing to prevent payments that violated sanctions. The same year, Schlumberger Oilfield Holdings was fined $232 million by the US Department of Justice (DOJ) for "wilfully facilitating illegal transactions and engaging in trade with Iran and Sudan".

While the prospect of incurring regulatory fines is a major concern, some of the other consequences of failing to implement suitable controls can, in some cases, be even more serious. Depending on the nature of the regulatory action, the company's business activities and earnings may be affected. For example, forfaiting house Deutsche Forfait lost 94% of its revenues in the space of a year after being placed on the OFAC SDN list for violating oil sanctions against Iran. Another concern is that media coverage of breaches in compliance can lead to significant and lasting reputational damage.

Taking compliance to the next level

Against this backdrop, companies are becoming increasingly aware of the risks of breaching regulatory compliance requirements. Viewing compliance as the responsibility of the company's banks is no longer sufficient. In order to make sure they are not doing business with sanctioned entities, or to prevent their business being used to launder illicit funds, companies are finding they need to adopt their own compliance solutions.

High-profile enforcement actions include PayPal's $7.7 million fine for failing to prevent payments that violated sanctions, and Schlumberger Oilfield Holdings' $232 million fine for "engaging in trade with Iran and Sudan".

These include name screening filters to screen customers and suppliers during onboarding and on an ongoing basis, as well as the growing deployment of transaction screening filters to screen transactions as these are sent to their banks for processing.

While some corporates have implemented strong controls for years, others may require a considerable change in mindset, particularly in organisations that continue to view such controls as the responsibility of their banks. Compliance solutions can represent a considerable departure from the core competencies of organisations which have been in the business of selling products for many years. Such organisations will need to step outside their comfort zone in order to tackle compliance in a more proactive way. They may also need to work with outside experts as they bolster their compliance processes.

This article first appeared in the June edition of *Money Laundering Bulletin.*

DOJ Guidance

The new DOJ guidance for corporates includes sample questions that corporate compliance teams should consider on the following topics:

1. Analysis and Remediation of Underlying Misconduct
2. Senior and Middle Management
3. Autonomy and Resources
4. Policies and Procedures
5. Risk Assessment
6. Training and Communications
7. Confidential Reporting and Investigation
8. Incentives and Disciplinary Measures
9. Continuous Improvement, Periodic Testing and Review
10. Third Party Management
11. Mergers and Acquisitions (M&A)

The questions included in the document are largely not new material: the introduction notes that many have already appeared in other documents such as the United States Attorney's Manual and the United States Sentencing Guidelines.

As well as US-specific publications, the document also cites OECD publications such as the 2010 Good Practice Guidance on Internal Controls, Ethics and Compliance.

Understanding regulatory guidance

In this challenging regulatory climate, companies should welcome any insights into regulators' expectations. One notable development was the recent publication of a document by the US Department of Justice (DOJ), Evaluation of Corporate Compliance Programs. The document outlines a number of different factors which are taken into consideration by the Fraud Section when it evaluates corporate compliance programmes during a criminal investigation. This document is relevant not only for global corporates with operations or clients in the US, but also for companies looking for insight into how they might be scrutinised by their regulator.

While noting that each company has its own risk profile and solutions – and that the DOJ's Fraud Section does not use a rigid formula during its assessments – the guidance says that there are "common questions that we may ask in making an individualized determination."

The DOJ guidance document can be seen primarily as a reminder for corporates of the need to put an effective compliance programme in place. While it is primarily of interest for corporates operating in the US, the questions it features can be regarded as a more far reaching insight into the issues being looked at by regulators. Corporates should therefore take the time to review the relevant sections and consider whether any changes are warranted in their own operations.

What does the document include?

The earlier sections focus on topics such as the root cause of the misconduct in question, the actions taken by senior leaders to discourage misconduct and the experience and qualifications of the company's compliance and control personnel. Other topics focus on the training provided to employees in the relevant control functions and the way in which the company's reporting mechanism is used.

In addition, the guidelines explore the need for companies to adopt suitable controls and test the effectiveness of those controls, based on several important principles.

Policies and procedures

This section includes questions on the company's process for designing and implementing new policies and procedures, and whether the company had policies and procedures in place that prohibited the misconduct. Focusing on operational integration, questions are included on who in the business has been responsible for designing, implementing and integrating policies and procedures, as well as asking about the absence or failure of controls which could have detected or prevented misconduct. Questions are also included on how the misconduct was funded and, if vendors were involved in the misconduct, what the company's process is for vendor selection.

The recent 'Evaluation of Corporate Compliance Programs' publication by the US Department of Justice (DOJ) provides companies with insight into how they might be scrutinised by their regulator.

Continuous improvement, periodic testing and review

The topics covered in this section include internal audit and whether relevant findings and remediation progress have been reported to management and the board on a regular basis. This section also focuses on control testing and whether the company has "reviewed and audited its compliance program in the area relating to the misconduct", including the testing of relevant controls, collection and analysis of compliance data, and interviews with employees and third parties.

In addition, questions are included on the topic of 'Evolving Updates'. These delve into how often the company has updated its risk assessments and reviewed its compliance policies, procedures, and practices, as well as the steps that the company has taken to "determine whether policies/procedures/practices make sense for particular business segments/subsidiaries".

Third party management

The questions in this section focus on how the company's third-party management process corresponded to the "nature and level of the enterprise risk identified by the company" and how this process has been integrated into the relevant procurement and vendor management processes. Questions are also included on the business rationale for the use of third parties and the mechanisms used to "ensure that the contract terms specifically described the services to be performed".

Lessons for corporates

These sections of the DOJ document have a number of implications for corporate compliance programmes. For one thing, the emphasis on the need for suitable controls indicates that corporates should consider whether they have adequate filters in place and should look critically at the level of trust that is warranted for third parties. Likewise, the focus on control testing underlines the need for corporates to ensure that their filters are effective, and to be able to demonstrate this effectiveness to regulators.The questions also highlight the need for companies to update their risk assessment measures and review their compliance policies, procedures and practices. As such, companies should pay close attention to the risks that they face in different jurisdictions, as well as considering what controls they need to put in place as the organisation grows geographically.

The emphasis on the need for suitable controls indicates that corporates should consider whether they have adequate filters in place and should look critically at the level of trust that is warranted for third parties.

Where third party management is concerned, many corporations appoint third parties to undertake certain compliance activities on their behalf, whether that means using tools provided by a service bureau to support an in-house team or outsourcing a significant part of the company's compliance department. In either case, the DOJ guidance highlights the need for companies to understand the level of compliance that third parties have in place, reinforcing the need for quality assurance systems.

Taking ownership

While most of the questions listed in the DOJ guidance may not be new material, the document is nevertheless a powerful illustration of what regulators, especially US regulators, are looking at when evaluating a corporate's compliance programme. It is also illustrative of the measures companies should be taking in order to meet compliance requirements and reduce the risk that they will be the subject of regulatory actions.

In the current regulatory environment, it is essential that corporates take the necessary steps to comply with applicable regulations and mitigate regulatory and reputational risk. While some companies still regard compliance as a bank controlled process, others are taking ownership of this area by undertaking activities such as name and transaction screening and using external vendors to support their compliance activities. Corporates which have not yet done so should consider implementing robust controls which can protect their businesses from the risks of non-compliance.

Supporting corporate compliance

SWIFT provides a number of products which help corporates to comply with sanctions screening requirements.

Sanctions Screening
A fully managed service which screens incoming and outgoing messages against the latest sanctions lists and alerts users to any matches. Different workflow options can be used to fit the company's processes.

Name Screening
Corporates can use this service to check the names of suppliers and customers against sanctions, PEP and private lists, either during the onboarding process or when carrying one-off checks. The service also includes automatic list updates and a robust case management system.

Sanctions Testing
Sanctions Testing delivers independent quality assurance of corporates' transaction, customer and PEP filters. The service assesses filter models and automates sanctions testing and tuning, as well as making sure that lists are correct and up-to-date.

www.swift.com/complianceservices

About SWIFT

SWIFT is a global member owned cooperative and the world's leading provider of secure financial messaging services. We provide our community with a platform for messaging and standards for communicating, and we offer products and services to facilitate access and integration, identification, analysis and regulatory compliance.

Our messaging platform, products and services connect more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories. While SWIFT does not hold funds or manage accounts on behalf of customers, we enable our global community of users to communicate securely, exchanging standardised financial messages in a reliable way, thereby supporting global and local financial flows, as well as trade and commerce all around the world.

As their trusted provider, we relentlessly pursue operational excellence; we support our community in addressing cyber threats; and we continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies. Our products and services support our community's access and integration, business intelligence, reference data and financial crime compliance needs. SWIFT also brings the financial community together – at global, regional and local levels – to shape market practice, define standards and debate issues of mutual interest or concern.

Headquartered in Belgium, SWIFT's international governance and oversight reinforces the neutral, global character of its cooperative structure. SWIFT's global office network ensures an active presence in all the major financial centres.

www.swift.com/complianceservices

57286 - June 2017