Deloitte.

Finding the Holy Grail:

Driving effective FCPA compliance with advanced management controls and ISO 37001

The compliance demands imposed on businesses by the US Foreign Corrupt Practices Act (FCPA) have evolved and expanded over the FCPA's nearly 40-year existence, the change intensifying since the turn of the century. Enacted in 1977 in response to disclosures of widespread bribery of public officials by US companies and affiliates, the FCPA establishes civil and criminal penalties for illegal payments and sets standards for company internal controls to prevent and detect the risk of potential violations.

The relative maturity of FCPA compliance programs in companies has largely tracked that of compliance programs generally, with heavily regulated sectors such as aerospace and defense among early adopters. Today, case studies demonstrating the need for stronger FCPA controls can be found across the industry landscape. In the past several years, businesses as diverse as financial services, software, infrared technology, and infant formula all have seen sanctions for FCPA violations.[1]

Regulators charged with enforcing the FCPA provisions, the US Department of Justice (DOJ) and the US Securities and Exchange Commission (SEC), have signaled they expect companies to strengthen anti-bribery management systems, with a particular emphasis on preventive controls.

A Resource Guide to the U.S. Foreign Corrupt Practices Act, jointly published by the DOJ Criminal Division and SEC Enforcement Division in 2012, continues to provide the most definitive guidance regarding the FCPA's anti-bribery and accounting provisions, enforcement principles, penalties and sanctions, and other regulatory perspectives. Tools such as the SEC's Account Quality Model (AQM), which detects outliers and other red flags in financial statements, demonstrate regulators' growing use of advanced data analytics in enforcement, while reinforcing the message that companies can and should employ such technologies to strengthen their compliance controls.

[1] FCPA Cases, US Securities & Exchange Commission, http://www.sec.gov/spotlight/fcpa/fcpa-cases.shtml.

So what does having stronger FCPA controls mean, how does a company develop and deploy them, and what role can technology play? As is often the case, the answers to these questions will depend on the company's inherent risk profile – its geographic scope of operations, associated FCPA risks, resources, and overall enterprise compliance program maturity. Companies can benefit from understanding where they reside on the spectrum of FCPA compliance program maturity, the challenges that can impede compliance program development, and the "art of the possible" in deploying advanced compliance controls within a company's enterprise resource planning (ERP) system environment.

The evolution of FCPA compliance — progress, but with challenges

FCPA compliance is a multi-year journey for most companies, the exceptions being those that encounter regulatory enforcement proceedings that tend to accelerate the process. Companies typically follow a similar path in establishing FCPA compliance controls designed to conform to increasing expectations among regulators. Initial steps include establishing more-robust formalized policies, communications, codes of conduct, and whistleblower programs, often accompanied by online and in-person, localized, reinforcement training. Businesses may establish a dedicated compliance office or function initially or later in the evolution but that, too, inevitably is an integral part of the journey.

Building on this foundation, companies next often implement processes that establish greater rigor and forward-looking, preventive capabilities, such as risk assessments and due diligence procedures for the onboarding of third parties and periodic auditing and testing of transactions for compliance with anti-corruption policies. As programs evolve further, auditing and monitoring capabilities expand from sample testing to methodologies that incorporate advanced data analytic tools and other advanced techniques for auditing transactions.

Several issues can impede FCPA controls development, one being the inherently complex nature of global companies. Multinational companies can have multiple divisions and operating entities, each with its own ERP system. While it may be possible to implement controls across lines of business or throughout a particular country, the typical "patchwork quilt" of systems found in a global corporation make it a substantial challenge to establish consistent, coordinated controls across the breadth of the enterprise. Establishing systematized reviews and approvals required to prevent illegal payments only adds another layer of complexity.

Finally, a mismatch of risks and resources can constrain compliance efforts. Put simply, it is not uncommon for locales with the greatest potential for bribery to have the least sophisticated compliance capabilities, controls and systems.

Where controls currently reside in ERP systems

At a systems level, initiatives to strengthen FCPA compliance through increased automation inevitably involve adaptation of ERP controls in three particular areas:

- *Procure to pay* — ordering, receiving, and paying for items and services
- *Order to cash* — receiving a customer order, fulfilling it, and collecting payment
- *Record to report* — gathering operational information and preparing financial reports

In each of these areas, especially in the procure-to-pay process, enhanced automated controls can potentially help improve FCPA monitoring and compliance.

Many forward-looking companies are now embedding automated FCPA controls in and around ERP systems, a complex process that requires commitment, continuity, and investment. Not all ERP solutions are created equally, and the path a company takes will hinge on the sophistication of its particular system. In general, the range of retrospective automated controls now available for FCPA compliance includes but is not limited to the following:

Automated training program monitoring — electronic tracking to determine who has and who has not received FCPA compliance training

- *Automated triggers for high-risk transactions* — duplicate payments, round-dollar payments, and cash distributions are among the factors that can trigger automatic referral of transactions for compliance review prior to payment.
- *Red-flag analysis* —monitoring of general ledger accounts for anomalies and suspicious transactions.
- *Electronic audit trails* — post-transaction monitoring to provide better evidence of compliance with company policies and procedures, including confirmation that required transaction approvals have been obtained and routed to the proper persons, and access and changes to electronic data are properly recorded.

These methods of automated compliance monitoring are available and being implemented today by companies across a host of industries. Yet still on the horizon is what's considered the Holy Grail of FCPA compliance — continuous monitoring of accounts and transactions using crawling software to identify and stop improper payments before they occur. That's hard to do, even for companies with sophisticated compliance programs and a strong level of ERP system controls in place. Payment approval may ultimately be a human judgment call, and multiple and complex layers of approval for every payment in the system could have the potential to bring business to a halt. Still, certain subsets of high-risk transactions can be subjected to enhanced measures such as advanced approval and quick post-transaction reviews to forge a path forward on the journey to continuous monitoring.

Starting with the basics

Happily, companies have at their ready disposal the recent 2016 guidance of the International Organization for Standardization (ISO) to guide them in the journey to implementation of advanced management controls. The recently published guidance contained in ISO 37001 ("Anti-Bribery management systems — Requirements with guidance for use) contains an essential list of anti-bribery controls that are "applicable to small, medium, and large organizations in all sectors" and recommends, among other things, the following foundational financial controls[2]:

1. Effective segregation of duties
2. Defined delegations of authority
3. Validation of required approvals
4. Countersignature requirements for payment approvals
5. Submission of supporting documentation
6. Stringent controls on cash
7. Detailed requirements for transaction descriptions
8. Management review of significant transactions
9. Independent financial audits and transaction testing

[2] http://www.iso.org/iso/iso37001

FCPA compliance tools for a global marketplace

Multinational companies can expect continued, if not intensifying, scrutiny of transactions and relationships by authorities seeking to thwart official bribery and level the commercial playing field. Opportunists, meanwhile, will continue stepping over the line, illicitly currying favor with authorities to secure prized business. Strengthening basic FCPA controls and accelerating the use of automated monitoring tools and continuing efforts to prevent improper payments can help companies enhance their financial well-being, business reputation, and potential for growth and success — and show authorities and stakeholders that they are committed to doing business the right way.

Contacts

Rob Biskup
Managing Director | Deloitte Advisory
Forensics & Investigations
Deloitte Financial Advisory Services LLP
+1.313.396.3310
rbiskup@deloitte.com

Samantha Parish
Principal | Deloitte Advisory
Forensics & Investigations
Deloitte Financial Advisory Services LLP
+1.415.783.4930
saparish@deloitte.com

Deloitte.