Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

By Tom Fox

Internal Controls in an FCPA Compliance Program

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives.

For more information, visit www.complianceweek.com.

Table of Contents

Author's Note

Internal controls have long been an overlooked requirement under the U.S. Foreign Corrupt Practices Act. This book continues my series of short works designed to provide clear and useful guidance to the compliance practitioner on a topic specific to anti-corruption compliance. Thanks to Matt Kelly, editor at Compliance Week, for providing me with a platform to publish my book, Aarti Maharaj, digital content editor at Compliance Week, for the assistance on style and content and my heart-of-gold wife, Michele, for editing it.

About the Author

Thomas Fox has practiced law for more than 30 years. He has been a trial lawyer in private practice, a general counsel in the corporate world, and is recognized as one the leading experts on the Foreign Corrupt Practices Act (FCPA) and compliance programs relating to both the FCPA and other anti-corruption laws.

He is the author of two prior award-winning books on the *FCPA: Lessons Learning on Compliance and Ethics and Best Practices Under the FCPA* and *UK Bribery Act*. He blogs daily on all things FCPA on his award winning blogsite, The FCPA Compliance and Ethics Blog, and podcasts on all things anti-corruption on The FCPA Compliance and Ethics Report. Fox writes for a variety of anti-corruption compliance magazines and publications, and is a featured columnist for Compliance Week. He can be reached at tfox@tfoxlaw.com.

Part I – What are internal controls?

The Securities and Exchange Commission is generally charged with protecting U.S. investors in publicly traded companies. This mandate extends to the fight against bribery and corruption as embodied in the Foreign Corrupt Practices Act (FCPA). The more notable (and painful) part of FCPA enforcement are the criminal provisions against bribery, administered by the Justice Department. The less notable part of the FCPA, however, are its books-and-records provisions administered by the SEC—and they are just as real of a risk to companies as the criminal part of the law.

The risk is simple: if a company is making illegal payments in the form of bribes or other corrupt payments, almost by definition it is not identifying such illegal activity on its books and records. What's more, the company does not have appropriate internal controls to prevent, detect, and remedy such illegal conduct. That sloppy record-keeping is what the books-and-records provisions of the FCPA address, and weak internal controls are what can put a company in that jeopardy.

Internal controls are therefore viewed as the foundation of any effective anti-corruption compliance program. But what specifically are internal controls in a U.S. Foreign Corrupt Practices Act (FCPA) compliance program? The starting point is the law itself. The FCPA requires the following:

> Section 13(b)(2)(B) of the Exchange Act (15 U.S.C. § 78m(b)(2)(B)), commonly called the "internal controls" provision, requires issuers to:
>
> Devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that—
>
> 1. Transactions are executed in accordance with management's general or specific authorization;
> 2. Transactions are recorded as necessary: (i) to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements, and (ii) to maintain accountability for assets;
> 3. Access to assets is permitted only in accordance with management's general or specific authorization; and
> 4. The recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences…

Internal controls are therefore viewed as the foundation of any effective anti-corruption compliance program

The Justice Department and the Securities and Exchange Commission (SEC), in their jointly released FCPA Guidance from 2012, state: "Internal controls over financial reporting are the processes used by companies to provide reasonable assurances regarding the reliability of financial

reporting and the preparation of financial statements. They include various components, such as: a control environment that covers the tone set by the organization regarding integrity and ethics; risk assessments; control activities, that cover policies and procedures designed to ensure that management directives are carried out (e.g., approvals, authorizations, reconciliations, and segregation of duties); information and communication; and monitoring."

Moreover, the design of a company's internal controls "must take into account the operational realities and risks attendant to the company's business, such as: the nature of its products or services; how the products or services get to market; the nature of its work force; the degree of regulation; the extent of its government interaction; and the degree to which it has operations in countries with a high risk of corruption."

A company should take the results from its risk assessment tools and then design a robust internal controls system based on its highest-risk factors

Aaron Murphy, a partner at the law firm Foley & Lardner and author of an excellent resource, *Foreign Corrupt Practices Act: A Practical Resource for Managers and Executives,* defines internal controls as "policies, procedures, monitoring, and training that are designed to ensure that company assets are used properly, with proper approval and that transactions are properly recorded in the books and records. While it is theoretically possible to have good controls but bad books and records (and vice versa), the two generally go hand-in-hand–where there are record-keeping violations, an internal controls failure is almost presumed because the records would have been accurate had the controls been adequate."

Internal controls expert Henry Mixon describes internal controls as systematic measures—reviews, checks and balances, methods and procedures, and the like—instituted by an organization to perform several different functions. These functions allow a company to conduct its business in an orderly and efficient manner:

- Safeguard its assets and resources;
- Detect and deter errors, fraud, and theft;
- Assist an organization ensuring the accuracy and completeness of its accounting data, to let a business produce reliable and timely financial and management information; and
- Help an entity to ensure that employees, applicable third parties, and others all adhere to its policies and plans.

Mixon adds that internal controls can be "entity-wide," meaning that they are not just limited to accountants and auditors. Mixon also notes that for compliance purposes, controls are those measures specifically intended to provide reasonable assurance any assets or resources of a company cannot be used to pay a bribe. This definition includes diversion of company assets, such as

by unauthorized sales discounts or receivables write-offs or the distribution of assets.

The FCPA Guidance goes further to specify that internal controls are a "critical component" of a *best practices* anti-corruption compliance program. This is because the design of an entity's internal controls "must take into account the operational realities and risks attendant to the company's business, such as the nature of its products or services; how the products or services get to market; the nature of its work force; the degree of regulation; the extent of its government interaction; and the degree to which it has operations in countries with a high risk of corruption. A company's compliance program should be tailored to these differences." In other words, a company should take the results from its risk assessment and design a robust internal controls system based on its highest-risk factors.

In the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) publication, *Internal Controls – Integrated Framework* (hereafter the "Integrated Framework"), it noted that after a company analyzes its own risk, through a risk assessment, it should design its most robust internal controls around its highest risk. The Integrated Framework went on to define risk as the possibility that an event can happen and harm the objectives of an organization. A risk assessment, therefore involves a dynamic and iterative method for identifying and assessing threats. Compliance risks throughout a company are considered relative to established risk management techniques. Thus, risk assessment forms the basis for determining how risks will be managed. But this risk management must also consider external changes, which might render internal compliance controls ineffective.

A risk assessment therefore involves a dynamic and iterative method for identifying and assessing threats

Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance. This definition reflects certain fundamental concepts. Internal control is (italics taken directly from COSO, followed by my thoughts):

- **Geared to the achievement of objectives** in one or more categories: operations, reporting, and compliance;
- **A process consisting of ongoing tasks and activities:** A means to an end, not an end in itself;
- **Effected by people:** Not merely about policy and procedure manuals, systems, and forms, but about people and the actions they take at every level of an organization to affect internal control;
- **Able to provide reasonable assurance:** Rather than *absolute* assurance, provided to an entity's senior management and board of directors;
- **Adaptable to the entity structure:** Flexible in application for the entire entity or for a

particular subsidiary, division, operating unit, or business process.

The *Integrated Framework* even admits that its definition "is intentionally broad. It captures important concepts that are fundamental to how organizations design, implement, and conduct internal control, providing a basis for application across organizations that operate in different entity structures, industries, and geographic regions."

Why are internal controls important in your FCPA compliance program? Three recent FCPA enforcement actions demonstrate the reason.

The first came in late 2013, when the Justice Department obtained a criminal plea from Weatherford International. Weatherford failed to institute appropriate internal controls around three areas. First were controls on its third parties and business transactions, limits of authority, and documentation requirements. Second were controls for evaluating business transactions effectively, including acquisitions and joint ventures (JVs), for corruption risks and for investigating those risks when detected. Last were controls on excessive gifts, travel, and entertainment, where such expenses were not adequately vetted to ensure that they were reasonable, bona fide, and properly documented.

The second case arose in September 2014 involving the gun manufacturer Smith & Wesson (S&W). The case did not include a criminal charge filed by the Justice Department, only a civil matter prosecuted administratively by the SEC. In its administrative order, the SEC faulted S&W's internal controls for international sales operations: While the company had a basic corporate policy prohibiting the payment of bribes, "it failed to implement a reasonable system of controls to effectuate that policy."

Moreover, the company did not "devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that transactions are executed in accordance with management's general or specific authorization; transactions are recorded as necessary to maintain accountability for assets, and that access to assets is permitted only in accordance with management's general or specific authorization."

Finally in November 2014 was the Bio-Rad FCPA enforcement action. In that case there was clear evidence that bribes were paid, yet no criminal enforcement action was taken against the company as it received a non-prosecution agreement (NPA) from the Justice Department. The failure of internal controls, however, was found in three different bribery schemes in three separate countries. The SEC cease and desist order stated, "although it [Bio-Rad] had an ethics policy prohibiting the payment of bribes and various policies and procedures requiring accurate books and records, its systems of internal controls proved insufficient to provide reasonable assurances that such payments would be detected and prevented."

The whole concept of internal controls is that companies need to focus their efforts *where the*

risks are–whether they are compliance risks or others—and then allocate their limited resources to putting controls in place that address those risks. In the anti-corruption world, of course, your two big risks lie in the assets or resources of a company. Cash can always be used to pay a bribe, but so can inventory or other fixed assets. The second big vehicle for corruption is diversion of company assets, such as unauthorized sales discounts or receivables and write-offs, which might be used to pay a bribe.

The second big vehicle for corruption is diversion of company assets, such as unauthorized sales discounts

As an exercise, I suggest that you map your existing internal controls to the Justice Department and SEC's November 2012 release: *A Resource Guide to the U.S. Foreign Corrupt Practices Act* (herein the "FCPA Guidance") formulation of the "Ten Hallmarks of an Effective Compliance Program" (or some other well-known anti-corruption regime) to see where control gaps may exist. That understanding of your gaps will, in turn, help you determine whether or not you have adequate internal controls for FCPA compliance. From there you can proceed to determining whether those controls actually work and "functioning."

Internal controls will only become more important in FCPA enforcement. You need to get ahead of the curve. Indeed, in May 2015, the SEC announced an FCPA enforcement action against BHP Billiton, where there was no evidence the company violated the FCPA by paying bribes around its hospitality program provided to foreign governmental officials to the 2008 Beijing Olympics. Yet the company paid the second highest fine on record to the SEC— $25 million— for insufficient internal controls. This was different from the Smith & Wesson enforcement action, where Smith and Wesson was fined for not having the appropriate internal controls.

I. Internal Controls for Gifts, Travel and Entertainment

One reasonable expectation is that internal controls over gifts would be designed to ensure that all gifts satisfy the criteria as defined and interpreted in company policies. Generally speaking, these are fairly narrow, including a clear definition of the dollar limit for permissible gifts, coupled with some subjective criteria such as the legality of the gifts for the recipient and identifying whether the practice is customary within the country where the gift is delivered. The question I focus on is how to enforce these policies so that employees are not free to disregard them at will.

Through several enforcement actions and the FCPA Guidance, the Justice Department has emphasized the importance of risk assessment and effective controls and building a program tailored to those risks. Many companies effectively minimize the risk of inappropriate gifts through

stringent pre-approval requirements. In many cases, a sufficiently robust and enforced pre-approval policy can reduce the number of gifts presented simply because of the extensive pre-approval process. This has the added benefit of ensuring enforcement of internal controls, largely because of the reduced volume of gifts being included in expense reports.

Many companies effectively minimize the risk of inappropriate gifts through stringent pre-approval requirements

Mixon cautions that in considering the effectiveness of controls, you must always keep in mind the most common method for defeating an internal control driven by a dollar-amount criteria: splitting the whole item into multiple parts, so that each appears to stay under the limit and avoid the defined approval authority based on the amount of the gift.

The key analysis is whether controls are in place to enforce the policies and whether those controls are documented. To help to answer this question, Mixon posits four issues to evaluate:

1. Is the correct level of person approving the payment or reimbursement for the gift?
2. Are there specific controls, including sign-offs, to demonstrate that the gift had a proper business purpose?
3. Are the controls regarding gifts sufficiently preventative, rather than relying on detective controls?
4. If controls are not followed, is that failure detected by other internal controls or compliance protocols?

While many compliance practitioners believe that employee expense reports are a sufficient internal control regarding gifts, tighter controls should be in place because gifts can be presented in many other ways. Once your company policy on gifts has been finalized, the internal controls over expense reports fall into three basic areas:

1. The expense report format, including what information it requires;
2. Controls over the submitting employee and the preparation of the expense report; and
3. Controls to ensure the approvers conduct their reviews properly.

Even just the format of an expense report can go a long way in preventing violations of a company's policy. First, have preprinted representations and certifications within the form, since these can lead to "stop and think" controls, meaning the person submitting the expense report must at least consider the information being submitted. The form can be signed without reading the preprinted representations, but if the employee and reviewers have been trained on how to review the expense report, it can be difficult to prove that the submitting employee did not understand what he was signing.

Two forms of representation can operate as internal controls: preparer's representations, and the

approver's representations. The preparer's representations include ensuring that all items representing a proper business purpose comply with the company's Code of Conduct, local law and customs, and all applicable company policies regarding FCPA compliance. The approver's representations ensure that all supporting documentation has been carefully examined and that all documentation complies with applicable company policies, including the submission of original receipts. Further, the approver should certify that the employee complied with all of the company's policies regarding the review and approval of the expense report.

Many companies have two basic forms of expense reports. One is for situations where all items pertain to U.S. locations and do not involve any expenses incurred outside of the United States, or expenses incurred for the benefit of anyone outside the United States. The second is for items involving locations or persons beyond U.S. borders. The international reporting form may have more stringent requirements and should provide more detailed disclosures. It could require reporting, in a separate section of the expense report, all items that involve government officials, so that these items are not "buried" elsewhere in the expense report.

The approver should certify that the employee complied with all of the company's policies regarding the review and approval of the expense report

As an added measure, the expense report can include a column where other expenses are reported and require the submitter to check "Government Official Y/N". This type of format should require sufficient disclosure of information regarding each item involving government officials.

The next step in such an enhanced protocol would require a senior officer from the business unit to approve any reimbursements that meet certain criteria—for example, certain geographical areas or countries. Finally, such an enhanced representation could also include separate sections for each item requiring a description of the business purpose of meals, entertainment, names, and business affiliation of all attendees and description of gifts. A typical expense report requires this information to be on the receipt.

Moving beyond simply requiring receipts, to asking for such detailed reports, underlines the presence or absence of proper documentation in advance. Moreover, that documentation is crucial to ensure that reviewers can properly sign off each item as having the necessary documentation and pre-approvals.

Companies must also beware of corporate checks and wire transfers, in response to falsified supporting documentation such as check requests, purchase orders, or vendor invoices. The Delegation of Authority (DOA) is a critical internal control here. For example, a wire transfer of $*X* between company bank accounts in the United States might require approval by the finance manager and one officer at the initiating location. A wire transfer of the same amount to the company's bank account in Nigeria, however, could require approval by the finance

manager, a knowledgeable person in the compliance function, and one officer. The key is that the DOA should specify who must give the final approval for such an expense.

A possible area for FCPA violations occurs where checks are drawn on local bank accounts in locations outside the United States in "off the books" bank accounts, commonly known as slush funds. Some petty cash funds outside the U.S. have small balances, but substantial throughput of transactions. In these scenarios, your DOA should address the replenishment of petty cash funds in countries outside the United States, as well as approval of expense reports for employees who work outside U.S. borders, including those who travel from the United States to work outside the country.

Travel is another area for concern, since a company's corporate travel department and independent travel agencies can buy tickets, hotel rooms, and the like for non-employees. Internal controls might be needed to ensure policies are enforced when travel for non-employees can be purchased through a corporate travel department or through independent travel agencies.

However, it is not simply corporate travel departments that pose the compliance risk in this situation. As was demonstrated with GlaxoSmithKline in China—where GSK was fined $490 million by Chinese authorities in 2014 for various bribes executed under the guise of working with outside travel agents—a company must not discount the risk related to the abuse of power internally and collusion with independent travel agencies. In the GSK matter, the business unit managers in China paid bribes to Chinese government officials through independent travel agencies. GSK demonstrates that a company should implement procedures to ensure management is in compliance with its company's policies regarding payment of travel and related expenses for third parties.

Procurement or "P cards" cards have long been an area for fraud, corruption and corporate abuse

Procurement or "P cards" cards have long been an area for fraud, corruption and corporate abuse. If your company uses procurement cards, assume this to be a high-risk area, not just for FCPA but also for fraud risk generally. Banks have made a great selling job to corporations for the use of P cards to help to facilitate "cash management," but more often than not, they can simply be a streamlined way to allow embezzlement and misbehavior to go undetected. A control objective should be put in place along the lines of written policy and procedures defining the acceptable and unacceptable use of company P Cards, required forms, required approvals, documentation, and review requirements.

Internal controls expert Mixon uses an interesting analogy in this area: that *misbehavior, like water, seeks its own level*. This means if the pre-approval process and strong controls over expense reports prevent misbehavior, employees who wish to misbehave will seek other ways to do it, especially where controls are not so strong. You should use your risk assessment to help

prioritize where controls are most needed.

If your company prohibits gifts and any travel (other than for the submitting employee) from being included in the expense report, you should consider requiring that a check request form be used, which would be subjected to stringent controls. In such cases, a checklist should be completed and attached to the check request form that includes questions and disclosures designed to flesh out exactly what was provided in the business class airline, pocket money, event tickets, side trips, leisure activities, spouses or other relatives who might be traveling, and why the travel had a business purpose. Such internal controls would allow a more streamlined processing of expense reports and still elevate the gifts/travel items to the appropriate level of review.

While a compliance officer might rely on internal audit processes regarding gifts, it is important to keep in mind that, with respect to gifts, internal audits most often constitute—at best—a detective control that only gives comfort for some historical period. It is not necessarily representative of the controls in place to prevent future violations. So any compliance officer who depends on the internal audit of expense reports as effective internal control for FCPA risk is giving himself a false sense of security.

It is important to keep in mind that, with respect to gifts, internal audits most often constitute—at best—a detective control

II. Internal Controls for Third-Party Representatives

A compliance practitioner should analyze any third-party representative to understand the pattern of dealings with such third parties, and therefore the areas where additional controls might be warranted. There are some basic internal controls that should be a part of any financial controls system. The general internal controls, which might be appropriate, could be some or all of the following:

- A control to correlate the approval of payments made to contracts with third-party representatives and your company's internal system for processing invoices.
- A control to monitor all situations where funds can be sent outside the United States, in whatever form your company might use, which could include accounts payable computer checks, manual checks, wire transfers, replenishment of petty cash, loans, advances or other forms.
- A control for the approval of sales discounts to distributors.
- A control for the approval of accounts receivable write-offs.
- A control for the granting of credit terms to third parties or customers outside the United States.
- A control for agreements for re-purchase of inventory sold to third parties or customers.

- A control for opening of bank accounts specifically including accounts opened at request of an agent or a customer.
- A control for the movement or disposal of inventory.
- A control for the movement or disposal of movable fixed assets.
- Execution and modification of contracts and agreements outside the United States.

In addition to the above, some internal control needs are based on activities with third-party representatives. These could include some or all of the following:

- A control for the structure and enforcement of delegation of authority.
- A control for the maintenance of the vendor master file.
- A control around expense reports received from third parties.
- A control for gifts, entertainment, and business courtesy expenditures by third-party representatives.
- Charitable donations.
- All cash or currency, inventory, fixed asset transactions, and contract execution in countries outside the United States, where the country manager has final authority.
- Any other activity for which there is a defined corporate policy relating to the FCPA.

While that list may appear overly exhaustive, there are four significant controls, that a compliance practitioner can implement initially. They are:

1. DOA;
2. Maintenance of the vendor master file;
3. Contracts with third parties; and
4. Movement of cash or currency.

If the DOA is properly prepared and enforced, it can serve as a powerful preventive tool for FCPA compliance. It should incorporate the impact of FCPA risk, including both transactions and geographic locations, so that a higher level of approval for matters involving third parties and for fund transfers and invoice payments to countries outside the United States would be required inside an organization—even if your DOA is prepared without much thought about FCPA risks.

Unfortunately, once a DOA is prepared, it is not used again until it is time to update for personnel changes. Moreover, DOA controls are often not available, not kept current, or did not define authority in a way even the approvers can understand. Therefore it is incumbent that the DOA be integrated into a company's accounts payable (AP) processing system in a manner that ensures all high-risk vendor invoices receive the proper visibility. To achieve this, you should identify the vendors within the vendor master file, so payments are flagged for the appropriate approval *before* they are paid.

A vendor master file can be one of the most powerful preventive control tools, largely because

payments to fictitious vendors are one of the most common occupational frauds. The vendor master file should be structured so that each vendor can be identified not only by risk level, but also by the date on which the vetting was completed and the vendor received final approval. Electronic controls should be in place to block payments to any vendor for which vetting has not been approved.

Next, manual controls are needed over the submission, approval, and input of changes to the vendor master file. These controls include verification that all vendors have been approved before their information (and the vendor approval date) is added to the vendor master. Finally, manual controls are also needed when "one time" vendors are requested, and when a vendor name or vendor payment information changes are submitted.

Near and dear to my heart as a lawyer, contracts with third parties can be a very effective internal control to prevent nefarious conduct rather than to detect errors and abuses. For contracts to provide effective internal control, however, relevant terms of those contracts (commission rate, whether business expenses can be reimbursed, use of subagents, and so forth) should be extracted and available to those who process and approve vendor invoices. If there are nonconforming service descriptions, commission rates, etc., present in a contract, then such terms must be approved not only by the original approver but also by the person so delegated in the DOA. Unfortunately, contracts are not typically integrated into the internal control system, but rather are left off to the side on their own, usually gathering dust in the legal department file room.

Electronic controls should be in place to block payments to any vendor for which vetting has not been approved

The Hewlett-Packard 2014 FCPA enforcement action was an excellent example of the lack of internal control over disbursements of funds and movement of currency. In this case, you had the country manager delivering bags of cash to a Polish government official to pay for business. This cash had to come from somewhere. At some point, a second set of eyes on the Poland finances might have noticed that some petty cash was missing. This enforcement action demonstrates that all situations where funds can be sent outside the United States (AP computer checks, manual checks, wire transfers, replenishment of petty cash, loans, advances, and more,) should be reviewed from an FCPA-risk standpoint. It also shows that within a given company structure, you need to identify the ways in which a country manager (or a sales manager, business unit manager, and the like) could cause funds to be transferred to his control and to conceal the true nature of the use of the funds within the accounting system.

To prevent such misconduct, robust internal controls need to be in place. All wire transfers outside the United States should have defined approvals in the DOA, and the persons who execute the wire transfers should be required to show evidence agreement of the approvals to

the DOA. Wire transfer requests going out of the United States should *always* require dual approvals. Lastly, wire transfer requests going outside the United States should be required to include a description of proper business purpose.

I have said it before, but it bears repeating. Internal controls are really *just good financial controls*. The internal controls detailed for third-party representatives in the FCPA context will help to detect fraud, which could well lead to bribery and corruption. Given that third parties are almost universally recognized as your highest FCPA risk, you may well wish to assess that part of your internal control and compliance program first.

III. Board of Directors' Oversight as an Internal Control

Can a board of directors act as a compliance internal control? I think the clear answer is yes. In the FCPA Guidance, the "Ten Hallmarks of an Effective Compliance Program" there are two specific references to the obligations of a board in a best practices compliance program.

The first in Hallmark No. 1 states: "Within a business organization, compliance begins with the board of directors and senior executives setting the proper tone for the rest of the company." The second is found under Hallmark No. 3 (*Oversight, Autonomy and Resources*), which says that the chief compliance officer should have "direct access to an organization's governing authority, such as the board of directors and committees of the board of directors (e.g., the audit committee)." Further, under the U.S. Sentencing Guidelines, the board must exercise reasonable oversight on the effectiveness of a company's compliance program. And the Justice Department's Prosecution Standards posed the following queries:

1. Do the directors exercise independent review of a company's compliance program?
2. Are directors provided with sufficient information to exercise independent judgment?

The Justice Department's remarks drive home the absolute requirement for board participation in any *best practices* (or even just any effective) anti-corruption compliance program.

Board liability, for failure to perform its assigned function in any compliance program, is well known. David Stuart, a partner with Cravath, Swaine & Moore, in an article titled, "Surviving Scrutiny Through Best Practices" published in *Corporate Board Member*, noted that FCPA compliance issues can lead to personal liability for directors, as both the Securities and Exchange Commission and the Justice Department have been "very vocal about their interest in identifying the highest-level individuals within the organization who are responsible for the tone, culture, or weak internal controls that may contribute to, or at least fail to prevent, bribery and corruption."

Stuart pointed to the SEC's enforcement action in 2009 against two senior executives at Nature's Sunshine Products, as an example. There, the CEO and CFO were each ordered to pay a civil penalty of $25,000, in addition to the company itself paying a $600,000 penalty. Likewise, Stuart said, under certain circumstances, "I could see the SEC invoking the same provisions against audit committee members—for instance, for failing to oversee implementation of a compliance program to mitigate risk of bribery." The Nature's Sunshine enforcement action is significant because it was the first FCPA enforcement action where the SEC brought charges against two corporate officers, the CEO and CFO, who were not alleged to have engaged in bribery, only that they failed as control persons, violated the books and records and internal controls provisions of the FCPA. It would not be too far of a next step for the SEC to invoke the same provisions against audit committee members who do not actively exercise oversight of an ongoing compliance program.

Further, the SEC has made clear that it believes a board should take an active role in overseeing the management of risk within a company. The SEC has promulgated Regulation SK 407, under which each company must make a disclosure regarding the board's role in risk oversight. This "may enable investors to better evaluate whether the board is exercising appropriate oversight of risk." If this disclosure is not made, it could be a securities law violation and subject the company, to fines, penalties or profit disgorgement.

I believe that a board must not only have a corporate compliance program in place, but also oversee that function actively. Further, if a company's business plan includes a high-risk proposition, there should be additional oversight. In other words, the board has an affirmative duty to ask the tough questions. All this means more than simply having a compliance program in place. The board must exercise appropriate oversight of the compliance program and its function. The board needs to ask the hard questions and be fully informed of the company's overall compliance strategy going forward.

The internal controls detailed for third-party representatives in the FCPA context will help to detect fraud, which could well lead to bribery and corruption

Lawyers often advise boards on their legal obligations and duties. If a board's oversight is part of effective financial controls under the Sarbanes-Oxley Act, that also includes effective compliance controls. Failure to oversee either may result in something far worse than bad governance. It may lead to a FCPA violation and could even form the basis of an independent FCPA violation.

A company must not only have a corporate compliance program; it must also actively oversee that function. Failure to perform these functions may lead to independent liability of a board for its failure to execute its allotted tasks in an effective compliance program.

Internal controls work together with compliance policies and procedures. As stated by Murphy of Foley & Lardner, they are "an interrelated set of compliance mechanisms." He breaks

down internal controls into five concepts, which I have adapted for a board or board subcommittee role for compliance:

1. **Risk Assessment**: Boards should assess the compliance risks associated with its business.

2. **Corporate Compliance Policy and Code of Conduct**: Boards should have an overall governance document, which will inform the company, its employees, stakeholders and third parties of the conduct the company expects from an employee. If the company is global or multi-national, this document should be translated into the relevant languages as appropriate.

If a board's oversight is part of effective financial controls under the Sarbanes-Oxley Act, that also includes effective compliance controls

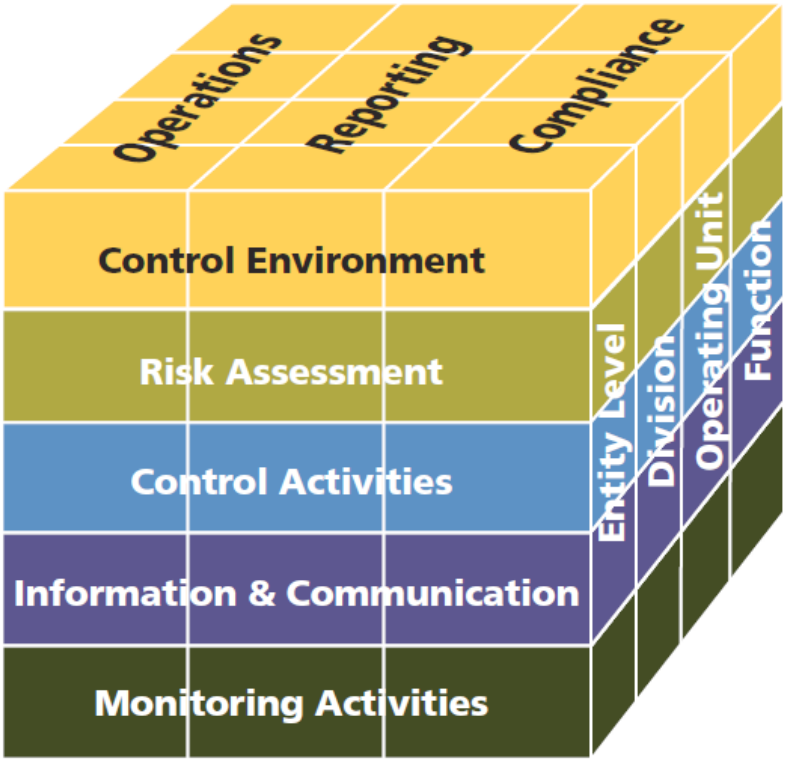
3. **Implementing Procedures**: Boards should determine whether the company has a written set of procedures in place that instructs employees on the details of how to comply with its compliance policy.

4. **Training**: Two levels of board training exist. The first should be that the board has a general understanding of what FCPA is; the second is that the board should also understand its role in an effective compliance program.

5. **Monitor Compliance**: Boards should independently test, assess and audit to determine if its compliance policies and procedures are a "living and breathing program" and not just a paper tiger.

I noted previously that as a basis for FCPA enforcement, there have been recent FCPA enforcement actions where the Justice Department and SEC discussed the failure of internal controls. For example, the questions around Walmart's board of directors and its failure to take action on allegations of bribery and corruption in the company's Mexico subsidiary, or failing even to be aware of these allegations, may lead to an independent basis for a FCPA violation based on the board's failure to perform its internal controls function in a *best practices* compliance program.

Part II - COSO and Internal Controls



What is COSO? The Committee of Sponsoring Organizations of the Treadway Commission (COSO), originally empaneled in 1987, adopted a framework in 1992 to design and test the effectiveness of internal controls. By 2012, a new generation of COSO members decided it was necessary to update the framework to reflect modern business practices. This more than 20-year old COSO Framework. In 2013 that new framework arrived, intended to be a supportable approach when anyone—regulators, litigants, investors, board directors, others—challenged whether a company has effective internal controls.

While the COSO 2013 framework is primarily used to build financial controls, COSO has been clear that the new framework is flexible and can be a roadmap for non-financial controls too. I believe that this flexibility will lead the SEC to use the 2013 framework to review a company's internal controls around compliance. This means that you need to understand what is required under the 2013 framework, and be able to show adherence to it or justify an exception—especially if you receive a letter from the SEC asking for evidence of your company's compliance with the internal controls provisions of the FCPA.

COSO has produced three volumes detailing the 2013 framework:

1. The first volume lays out the framework, "Internal Control – Integrated Framework" (herein "the Framework volume").

2. The second is an illustrative guide, "*Internal Controls – Integrated Framework, Illustrative Tools for Assessing Effectiveness of a System of Internal Controls*"—"the Illustrative Guide" which discusses how best to assess your internal control regime, and provides forms and worksheets to use in this exercise.

3. The third volume is an executive summary of the first volume, aptly titled "Executive Summary."

All three works form an excellent starting point for exploration of the COSO 2013 framework and how you might use it for your best practices FCPA anti-corruption compliance program.

The COSO model often portrays internal controls in the shape of a cube, from bottom to top, as follows:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring

In the 2013 update, the basic framework was retained while three specific objectives were added:

1. Operations: effectiveness and efficiency of operations, including safeguarding assets against loss;
2. Reporting: internal and external financial reporting; and
3. Compliance: adherence to laws and regulations to which the entity is subject.

According to guidance in the 2013 update, the system of internal controls can be considered effective only if it provides reasonable assurance that the organization, among other things, complies with applicable laws, rules, regulations and external standards. With the addition of those specific objectives, the COSO framework now specifically includes the need for controls to address compliance with laws and regulations.

Larry Rittenberg, a former chairman of COSO, in his book *COSO Internal Control-Integrated Framework* says that the original COSO framework from 1992 stood the test of time because "it was built as conceptual framework that could accommodate changes in: (a) the environment, (b) globalization, (c) organizational relationship and dependencies, and (d) information processing and analysis."

Working from that base, the updated 2013 Framework was structured upon four general principles:

1. The updated framework should be conceptual, which allows for updating as internal controls [and compliance programs] evolve;

2. Internal controls are a process designed to help businesses achieve their business goals;

3. Internal control applies to more than simply accounting controls—it applies to compliance controls and operational controls; and

4. While it all starts with tone at the top, "the responsibility for the implementation of effective internal controls resides with everyone in the organization." For the compliance practitioner, this final statement is of significant importance because it directly speaks to the need for you to be involved in the design and implementation of internal controls for compliance, and not to simply rely upon a company's accounting, finance or internal audit function to do so.

The primary point to keep in mind is that even if an organization adopts the framework, very few people within that organization will have the unique knowledge that a compliance officer has, that would touch all of the elements of the framework. The compliance officer's role is to provide the input to the chief financial officer and others involved in the implementation, to be sure that proper focus is on the risks that really are part of the compliance world. For example, the risk of sustaining a FCPA violation through the use of a third party who receives a commission based upon the final sales price is generally viewed as high. Conversely, the use of a third party to facilitate sales but who is compensated by an hourly rate is generally viewed as a much lower FCPA risk. This determination primarily comes through the risk assessment component, the control activities, and then the monitoring.

Companies typically do risk assessments from an operational standpoint. They address business risks going forward and then develop controls that deal with those business risks, such as forecasting financial results, doing business in certain countries, making strategic decisions, and similar issues. All of this puts the compliance function in a position to be the fulcrum upon which many issues will come up for a COSO-based analysis or implementation.

COSO's 5 Objectives and 17 Principles

In a 2013 Corporate Compliance Insights article, *The Updated COSO Framework: Time for a Fresh Look at Internal Control,* the author, Brian Christensen, says that the updated framework retained the core definition of internal controls: control environment, risk assessment, control activities, information and communication, and monitoring activities. Further, these five operational concepts are still visually represented in the well-known COSO Cube. In addition, the criteria used to assess the effectiveness of an internal control system remain

largely unchanged. The effectiveness of internal control is assessed relative to the five components of internal controls and the underlying principles supporting the components.

What's new is the emphasis on the principles that undergird the 2013 framework.

Christensen noted that COSO chose to formalize the principles from the 1992 version aid in the development of effective internal control and assessment of their effectiveness. While the 1992 version implicitly reflected the core principles of internal control, the 2013 Framework states them in the form of 17 principles, each of which is mapped to one of the five components. The 17 principles represent fundamental concepts associated with the five components of internal control.

The principles are broadly stated, as they are intended to apply to for-profit companies, not-for-profit entities, government bodies, and other organizations. Moreover, "supporting each principle are points of focus, representing features associated with the principles and providing guidance for their application. Together, they constitute the criteria and then the points of focus provide more specific guidance that will assist a company in assessing whether the components of internal control are present, functioning and operating together within the organization."

I. Control Environment

The first of the five components is the Control Environment. Rittenberg says the control environment "sets the tone for the implantation and operation of all other components of internal control." He adds that it starts with an ethical commitment from senior management, oversight by those in governance, and a commitment to competent employees. The five principles of the Control Environment are as follows:

1. Principle 1: The organization demonstrates a commitment to integrity and ethical values.

2. Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

3. Principle 3: Management establishes with board oversight, structures, reporting lines and appropriate authorizes and responsibility in pursuit of the objectives.

4. Principle 4: The organization demonstrates a commitment to attract, develop and retain competent individuals in alignment with the objectives.

5. Principle 5: The organization holds individuals accountable for their internal control responsibilities in the pursuit of the objective.

Principle 1 - Commitment to integrity and ethical values

What are the characteristics of this principle? First, and foremost, an entity must have the appropriate tone at the top of management for a commitment to ethics, compliance, and good business conduct. It also means that an organization establishes standards of conduct through the creation of a Code of Conduct or other foundational documents. The next step is to demonstrate that individual employees throughout the organization adhere to this standard. Finally, any deviations from the standard (bid rigging, fraud, bribery, harassment, and so forth) should be addressed by the company in a timely manner. From an auditing perspective, this means an auditor must be able to assess whether a company has met its ethics and compliance requirements and whether that commitment can be measured and assessed effectively.

Principle 2 - Board independence and oversight

This principle requires that a company's board of directors establish oversight of a compliance function, separate from the company's senior management so that it operates independently. Next, the board should have compliance expertise so it can manage the compliance function actively and intelligently. Finally, and perhaps most importantly, a board must provide oversight on all compliance control activities, risk assessments, compliance communications, and monitoring activities. Internal auditors must interact with a board's compliance committee (or other relevant committee such as the audit committee) to determine independence. There must also be documented evidence that the board's compliance committee provides sufficient oversight of the company's compliance function.

> The compliance officer's role is to provide the input to the chief financial officer and others involved in the implementation, to be sure that proper focus is on the risks

Principle 3 - Structures, reporting lines, authority and responsibility

This may not seem as obvious, but it is critical that a compliance reporting line go up to the board. Under this principle, you will need to consider all of the structures of your organization and then move to define the appropriate roles of compliance responsibility. Finally, this principle requires establishment of the appropriate authority within the compliance function. Your auditors must be able to assess whether compliance responsibilities are appropriately assigned to establish accountability in your organization for implementation, use of and remedy to any violations.

Principle 4 - Attracting, developing and retaining competent individuals

This principle gets into the practical details of doing compliance. It requires that a company establish compliance policies and procedures to implement the program it wants. Following this, there must be an evaluation of the effectiveness of those compliance policies and procedures, and any demonstrated shortcomings should be addressed. This principle hinges on the human component of a compliance program: a company must attract, develop, and retain competent employees for the compliance function. Lastly, a demonstrable compliance succession plan should be in place. A company must be able to show through its compliance policies and, equally importantly its actions, that it has a commitment to retaining competent employees who accept the company's general goal of doing business ethically and in compliance with the law.

Principle 5 - Individuals held accountable

This is the stick principle. A company must show that it enforces compliance accountability through its compliance up and down the chain of authority in it. To do so, a company must establish appropriate compliance performance metrics, incentives to do business ethically and in compliance, and finally, clearly reward such persons through a promotion or another incentive. Each employee must be evaluated on his or her compliance performance, coupled with both rewards and discipline for employee actions around compliance.

A board must provide oversight on all compliance control activities, risk assessments, compliance communications,and

This principle requires evidence that can prove to an auditor that processes exist to hold employees accountable to their compliance objectives. Conversely, if an employee does not fulfill the company's compliance objectives, he or she must face identifiable consequences. Also, if this accountability is not effective, the internal controls should be able to identify and manage the compliance risks.

II. Risk Assessment

The Integrated Framework recognizes that "every entity faces a variety of risks from external and internal sources." This component is designed to provide a company with a "dynamic and iterative process for identifying and assessing risks."

For the compliance practitioner, however, that will not sound new or even insightful. The

COSO Framework requires a component of management input and oversight that was perhaps not always well understood. The framework says that management specifies "objectives within the category relating to operations, reporting, and compliance, with such clarity to be able to identify and analyze risks to those objectives." For the compliance practitioner, this means you must be aware of changes in both the legal environment in which you operate outside the U.S. as well as the business environment. An example would be for those companies subject to the U.K. Bribery Act, which made facilitation payments illegal when the law became effective in 2011, were required to modify the compliance programs to accommodate this change in U.K. law.

This final requirement is also important for any internal controls relevant to anti-corruption controls. Changes are coming quite quickly in the realm of anti-corruption laws and their enforcement. Management needs to be cognizant of these changes and how they might affect its business model—particularly in the delivery of goods or services. Simply put, changes in the law, or in the enforcement of it, can increase your risk exposure. Compliance officers don't just need to know that fact in theory; they need to understand how it might affect them in practice.

The component of Risk Assessment consists of four principles. They are:

- Principle 6: "The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to the objectives."
- Principle 7: "The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed."
- Principle 8: "The organization considers the potential for fraud in assessment risks to the achievement of objectives."
- Principle 9: "The organization identifies and assesses changes that could significantly impact the system of internal control."

If an employee does not fulfill the company's compliance objectives, he or she must face identifiable consequences

Principle 6 – Suitable objectives

Your risk analysis should always relate to stated objectives. As noted in the framework, management is responsible for setting the objectives. Rittenberg explains that too often, an organization starts with "a list of risks, instead of considering what objectives are threatened by the risk, and then what control activities or other actions it needs to take." In other words, your objectives should form the basis on how you approach your risk assessments.

Principle 7 – Identifies and analyzes risk

Risk identification should be an ongoing process. Rittenberg believes that even though a risk assessment may originate at the top of an organization or perhaps an operating function, "the key is that an overall process exists to determine how risks are identified and managed across the entity." At all costs, siloed risks should be avoided. The framework cautions that risk identification "must be comprehensive."

Principle 8 – Fraud risk

Compliance practitioners should understand that fraud exists in every organization. The money generated to pay bribes can come from what may be characterized as "traditional" fraud schemes, such as employee expense accounts, fraudulent third-party contracting and payments, and even fraudulent over-charging and pocketing of the difference in sales price. This means that any type of fraud should be should be considered as an important risk analysis, not simply fraud as might relate to bribery and corruption solely. It is important that any company follow the flow of money and if the Fraud Triangle is present, management should be placed around such risk.

Principle 9 – Identifies and analyzes significant change

The cliché is that the only constant in business is change—which also happens to be true. The framework states, "every entity will require a process to identify and assess those internal and external factors that significantly affect its ability to achieve its objectives." Rittenberg says that companies "should have a formal process to identify significant changes, both internal and external, and assess the risks and approaches to mitigate the risk" in a timely manner.

Companies typically do risk assessment from an operational standpoint

III. Control Activities

COSO says that control activities these "are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to ensure that the achievement of objectives are carried out. Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment. They may be preventive or detective in nature, and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews. Segregation of duties is typically built into the selection and development of control activities. Where segregation of duties is not practical, management selects and devel-

ops alternative control activities." So the concept of a "second set of eyes" is directly enshrined in this objective.

As with the other components, however, control activities are not to be undertaken in a vacuum. Rittenberg says these activities "have traditionally received the most attention of the component" but notes that the real-world experience since the initial implementation of the COSO framework back in 1992 has demonstrated that "the effectiveness of control activities must be evaluated with the context of the other five components."

Moreover, he believes that these conditions are aided by a company's policies and procedures, which should help to lessen and manage risk going forward. Finally, control activities should be performed at all levels in the business process cycle within an organization.

The objective of control activities consists of three principles. They are:

- Principle 10: "The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels."
- Principle 11: "The organization selects and develops general control activities over technology to support the achievement of the objectives."
- Principle 12: "The organization deploys control activities through policies that establish what is expected and procedures to put policies into action."

"The Updated COSO Internal Control Framework" whitepaper emphasizes the inter-related nature of the five objectives as it notes that the risk assessment driven by the company's management provides a context for designing the control activities required to reduce risks to an acceptable level. Principle 10 relates to the selection and development of control activities that mitigate risk to the achievement of compliance objectives, Principle 11 speaks to technology and its role in achieving control activities and Principle 12 deals with the development of control activities through the establishment of policies and procedures.

Principle 10 - Selects and develops controls activities

Rittenberg notes that there is no "silver bullet" in selecting the right internal controls. Yet when combined with your risk assessment, this principle would point to an integration of your policies, procedures, and overall corporate responsibilities, which should be chosen "sufficiently to reduce the risk of not achieving the objectives to an acceptable level." You should consider your relevant business processes, evaluate your mix of control activities and then consider what levels within your organization they should be applied. Rittenberg cautions that

"controls should be assessed in relationship to the risk being mitigated" but companies should not simply employ a check-the-box approach by ticking off if controls are simply present. Always remember the final test is whether the controls are *effective*.

Principle 11 - Selects and develops general controls over technology

The COSO framework recognizes the relationship between the use of technology in business processes and compliance controls. Indeed, the use of technology will only increase and grow more important going forward. I would certainly expect the SEC to focus on a company's use of technology and the internal controls framework around the effectiveness of any technological solution in any evaluation of the company's overall compliance program. Therefore, under this principle you will need to determine not only how technology helps your compliance-related internal controls, but also the use of governance, risk, and compliance technology in your overall corporate business processes. To do so, you will need to consider your technology infrastructure around compliance internal controls and security management of the same. The information gathered from these processes should be used to move forward in implementing the most appropriate technology around your compliance internal controls.

> Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment

Principle 12 - Control activities established through policies and procedures

This principle should be the most familiar one to the compliance practitioner, as it points to the establishment of policies and procedures to support deployment of your compliance program. It also sets out the responsibility and accountability for executing policies and procedures, specifies and assures corrective action as required, and mandates periodic reassessment of activities. It also directs that competent personnel are in place to do all those tasks. Rittenberg adds that responsibilities for control activities "should be identified through policies and various procedures. Processes should be in place to ensure that all aspects are implemented and working."

While the objective of control activities should be the most familiar to the compliance officer, this objective demonstrates the inter-relatedness of all the five COSO objectives. Your control environment and risk assessment should lead you to this point. The control activities objective lays the groundwork for a living, breathing compliance program going forward.

IV. Information and Communication

COSO says information is necessary "for the entity to carry out internal control responsibilities to support the achievement of its objectives. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the other components of internal control."

Communication is the macro view. It means a continual process of delivering, distributing, and attaining information about your compliance program and its functioning. "Internal communication" refers to information *inside* your company, and how information is disseminated up, down, and across the business. Communication must be present to allow all employees to receive a clear message from senior management that internal control responsibilities are taken seriously. "External communication" is bilateral: it lets your company receive the inflow of relevant external information, and it provides important information to external parties in response to requirements and expectations. This is particularly important in the compliance arena around the issue of third-party risk management.

One of the more interesting aspects of this objective is that it runs both vertically and horizontally. Rittenberg says that information and communication "is not a one-way street: information needs to be generated at operational levels, and communicated across and up the organization to enhance decision-making." Moreover, he says, this means that while one or more senior managers might have the requirement to develop, create and implement policies and procedures; those policies and procedures must then be communicated downward in the organization, and feedback should go back to the top regarding the whole process. Rittenberg says, "information and communication must be fully integrated with the other components of the framework, most especially those of monitoring and risk assessment."

I would certainly expect the SEC to focus on a company's use of technology and the internal controls framework around the effectiveness of any technological solution

The component of information and communication consists of three principles. These are:

- Principle 13: "The organization obtains (or generates) and uses relevant, quality information to support the functioning of internal control."
- Principle 14: "The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control."
- Principle 15: "The organization communicates with external parties regarding matters

affecting the functioning of internal control."

In a white paper titled, The Updated COSO Internal Control Framework the author, Brian Christensen, states that the 17 principles are readily adaptable to compliance. I think they are more than simply adaptable; they provide a clear road map for the CCO or compliance practitioner on how to set up the right compliance controls. I believe that the SEC will measure your company's internal controls against these 17 principles, and if you cannot map your internal controls to them and provide audit evidence, you may well be in FCPA hot water.

Principle 13 – Use of relevant and quality information

"Internal communication" refers to information inside your company, and how information is disseminated up, down, and across the business

The framework makes clear that Principle 13 relates to *relevant* information and not simply reams upon reams of data. Rittenberg says, "Relevant, timely and quality information needs to be assessed by management and others to help identify" several areas within a company. For the compliance officer this means that you need to identify relevant data, which can be either internal or external.

The hard part is to transform that data to actionable information—for example, reviewing gift, travel and entertainment expenses from high-risk employees to find the truly errant or rogue employee, or studying large numbers of customer rebates or refunds to find kickbacks or bribes. Rittenberg also suggests that you need to consider the characteristics of the information and "whether or not such information is being used correctly and timely." The framework goes on to detail several categories of both internal and external information that can be good starting points for management to generate "useful information to relevant internal controls."

Principle 14 – Communications internally

This is the principle that brings the horizontal and lateral action required for information and communication. Rittenberg notes that Principle 14 relates to how information is communicated internally, but adds, "It is equally important that such information be communicated to those with responsibilities over operational and compliance objectives, as well as reporting objectives." Finally, he cautions that entities should assess whether there are any "gaps in the communication process."

Under Principle 14, therefore, you will need to determine several different things from the compliance perspective. Does the board communicate in a downward mechanism that gets its relevant instructions to the CCO or the compliance function? Does the CCO communicate upwards to the board? This principle clearly reinforces an access component for the compli-

ance function. But it also specifies the horizontal communication that I mentioned earlier to ensure that policies and procedures are effectively spread throughout an organization.

Principle 15 – Communications externally

This principle requires that a company communicate with relevant external parties. Rittenberg provides an excellent example when he cites the need for companies to communicate with third parties about relevant Codes of Conduct or similar documents, which might apply to them. He also points to the example of information about a hotline that could be provided to a third party to report any FCPA-related issues. But beyond a company sharing its relevant compliance information with contracted third parties (whether those parties are on the sales side or in the supply chain), Principle 15 recognizes that outside parties can "provide information to management on the effectiveness of internal controls … and regulatory communication."

Obviously communications lines must run in both directions, back and forth, from the compliance officer to the board—but Principle 15 requires more. An organization must have the capacity for dissemination of the appropriate compliance-related information to relevant third parties, such as agents on the sales side of an organization or vendors in the supply chain. For this principle, the compliance officer must therefore evaluate the communication lines to third parties. This communication can flow both ways, as noted earlier, with compliance obligations to third parties but also information in the form of compliance issues from these entities.

The information and communication element of COSO requires a wide range of information to go up and down the corporate chain. In a Corporate Compliance Insights article, *3 Challenging Principles in COSO's Framework: A Closer Look at Principles 2, 4 and 13* the author Ron Kral says that "people who understand the objectives, risks, and controls of the information flows necessary for accounting transactions and the preparation of financial statements are critical both on the side of management and the external auditor." This may require reliance on those with technical skills far greater than management can bring to bear.

Additionally, Kral says, "organizations may want to consider creating an inventory of information requirements (both from internal and external sources), maintaining written data flow processes, implementing robust controls over spreadsheets, maintaining sound data repositories and instituting a data governance program. This could range from simply documenting the length of your document retention policy to also implementing and testing the effectiveness of your documents hold policy when the need arises. A data governance program will go a long way towards establishing and communicating the necessary pillars for Information and Communication, including roles and responsibilities." Fortunately for compliance professionals, no single recipe exists for success, so you can bring a wide range of talents, skills and imagination to bear on this objective.

V. Monitoring Activities

The fifth component is Monitoring Activities. The Framework volume says, "Ongoing evaluations, built into business processes at different levels of the entity, provide timely information." This means you should have a program of regular evaluations, perhaps as often as annually but no less than biennially, combined with separate evaluations to test specific effectiveness of your overall internal controls. Here it might be easier to think of the ongoing evaluations as base line evaluations to test the overall effectiveness of your program and the separate evaluations could review specific components of your compliance program. For instance you may wish to test certain parts of your third party management program more often the once every two years or even annually. This objective also requires communication of the results up the chain to senior management and the board as appropriate.

The compliance officer must therefore evaluate the communication lines to third parties

As with all other components of the COSO Cube, monitoring activities are part of an inter-connected whole and cannot be implemented singularly. This objective "applies to all five components of internal control, and the nature of monitoring should fit the organization, its dependence on IT, and the effectiveness of monitoring providing relevant feedback on the other components, including the effectiveness of control activities," Rittenberg states.

I heartily agree with Rittenberg when he says that he believes monitoring will assume increased importance in the future. For compliance officers, monitoring actives have been growing in importance over the past few years and will continue to do so in the future. In the "Five Principles of an Effective Compliance Program," developed by Paul McNulty and Stephen Martin at the law firm Baker McKenzie, they listed oversight as Principle 5 (their fifth principle, not to be confused with the COSO Principle 5 mentioned earlier). That fifth principle includes ongoing monitoring, and it is reinforced in the 2013 COSO framework.

In a Corporate Compliance Insights article, *Implementing COSO's 2013 Framework: 10 Questions that Need to be Answered*, Ron Kral explains that it is important to "ensure that adequate controls are 'present' in support of all relevant principles and the components before launching into efforts to prove that the controls are "functioning." Remember that all relevant principles must be present and functioning for a company to safely conclude that their internal controls over financial reporting is effective. Aligning the design of controls to the 17 principles to see any gaps early in the implementation process will help ensure adequate time to remediate and test for operating effectiveness." The same is equally, if not more so, true for your company's compliance function.

The monitoring activities component consists of two principles. They are:

- Principle 16: "The organization selects, develops and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning."

- Principle 17: "The organization evaluates and communicates internal control deficiencies timely to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate."

Principle 16 – Ongoing evaluation

Rittenberg stresses that this principle requires that monitoring should include "ongoing or 'continuous monitoring' whenever such monitoring is reliable, timely and cost-effective." This clearly incorporates McNulty and Martin's dictate that Principle No. 5 consists of not only auditing but ongoing monitoring as well. The reason is simple; they are complementary tools to test the effectiveness of your compliance regime. The same is true of internal controls. But this principle clearly expects your organization to engage in both types of oversight, monitoring and auditing.

For compliance officers, monitoring actives have been growing in importance over the past few years and will continue to do so in the future

The compliance officer needs to consider several areas and concepts going forward from here. A current risk assessment or other evaluation of business changes should be considered based upon some type of baseline understanding of your underlying compliance risk. Whatever you select, it will need to be integrated with your ongoing business processes, adjusted as appropriate through ongoing risk assessments, and then objectively evaluated.

Principle 17 – Evaluation and communication of deficiencies

This final principle speaks to deficiencies and their correction. Rittenberg notes that it requires a determination of what might constitute a deficiency in your internal control system, who in your company is responsible for taking corrective action, and whether there is evidence that the corrective action was taken. If that does not sound like McNulty Maxim No. 3—"What did you do when you found out about it?"— I do not know what does.

Therefore, under this principle, the CCO will need to take timely and determined action to correct any deficiencies that might appear in your compliance regime. It will require you to

assess results, communicate the deficiencies up the chain to the board or audit committee, correct those deficiencies, and then monitor the corrective action going forward. Adapting Kral, I would urge that every key internal compliance control in support of the 17 Principles should "conclude upon by management in terms of their adequacy of design and operating efficiency."

The monitoring actives component should bring together your entire compliance program and give you a sense of whether it runs properly. Both ongoing monitoring and auditing are tools the compliance officer should use in support of this objective. Near the end of his section on this objective, Rittenberg states, "Monitoring is a key component of the internal control framework because effective monitoring: (a) recognizes the dynamics of change within an organization, and (b) provides the basis for corrective action on a timely basis." I would add that it allows you to evaluate the effectiveness of that corrective action as well.

A current risk assessment or other evaluation of business changes should be considered based upon some type of baseline understanding of your underlying compliance risk.

Part III - Assessing Compliance Internal Controls

In its Illustrative Guide, part of the COSO 2013 framework "*Internal Controls – Integrated Framework, Illustrative Tools for Assessing Effectiveness of a System of Internal Controls*" (herein 'the Illustrative Guide'), COSO laid out its views on "how to assess the effectiveness of its internal controls." It went on to note, "an effective system of internal controls provides reasonable assurance of achievement of the entity's objectives, relating to operations, reporting and compliance." Moreover, there are two over-arching requirements that can only be met through such a structured post. First, each of the five components must be present and function. Second, the five components must be "operating together in an integrated approach." One of the most critical components of the COSO framework is that it sets internal control standards against which you can audit to assess the strength of your compliance internal control. In this Section, using FCPA as an example, I will take a look at how you can perform such an audit and assessment to demonstrate compliance with the internal controls requirement.

As the COSO Framework is designed to apply to a wider variety of corporate entities, your audit should be designed to test your internal controls. This means that if you have a multi-country or business unit organization, you need to determine how your compliance internal controls are inter-related up and down the organization. The Illustrative Guide also realizes that smaller companies may have less formal structures in place throughout the organization. Your auditing can and should reflect this business reality. Finally, if your company relies heavily on technology for your compliance function, you can leverage that technology to "support the ongoing assessment and evaluation" program going forward.

The Illustrative Guide suggests a four-pronged approach in your assessment:

1. Make an overall assessment of your company's system of internal controls. This should include an analysis of "whether each of the components and relevant principles is present and functioning, and the components are operating together in an integrated manner."
2. There should be a component evaluation. In this case, you need deeply evaluate any deficiencies that you may find and determine whether any compensating internal controls exist.
3. Assess whether each principle is present and functioning. As the COSO framework does not prescribe "specific controls that must be selected, developed and deployed," your task here is to look at the main characteristics of each principle, as further defined in the points of focus behind each one. Then determine whether a deficiency exists and if so, what is the severity of the deficiency.
4. Finally, summarize all your internal control deficiencies in a log so they are addressed on a structured basis.

Another way to think through the approach could be along the following lines. A Principle Evaluation should consider "the controls to effect the principle" and would allow internal control deficiencies to be "identified along with an initial severity determination." A Component Evaluation would "roll up the results of the component's principle evaluations" and would allow a re-evalu-

ation of the severity of any deficiency in the context of compensating controls. Lastly, an overall Effectiveness Assessment would explore whether the controls were "operating together in an integrated manner by evaluating any internal control deficiencies aggregate to a major deficiency."

This type of process would lend itself to an ongoing evaluation, so that if business models, laws, regulations or other situations changed, you could assess whether your internal controls were up to the new situations or needed adjustments.

One of the most critical components of the COSO framework is that it sets internal control standards against which you can audit to assess the strength of your compliance internal control

The Illustrative Guide spends a fair amount of time discussing deficiencies. Initially, it defined an internal control deficiency as a "shortcoming in a component or components and relevant principle(s) that reduces the likelihood of an entity achieving its objectives."

It defines a *major* deficiency as an "internal control deficiency or combination of deficiencies that severely reduces the likelihood that an entity can achieve its objectives." Having a major deficiency is a significant issue because, "When a major deficiency exists, the organization cannot conclude that it has met the requirements for an effective system of internal control," says the Illustrative Guide.

Moreover, unlike routine deficiencies, "a major deficiency in one component cannot be mitigated to an acceptable level by the presence and functioning of another component." This means if you fail to implement a control around a high-risk scenario such as gifts, travel and entertainment, or fail to have effect controls around this area—that would be a major deficiency. For example, if you have no monitoring activities at all for your travel and entertainment spending, no amount of effort in the other four components will make up that difference. In contrast, if you only lack an internal control or have an ineffective segregation of duties around review of such expenditures, it could be remedied.

Under a compliance regime, you may be faced with known or relevant criteria to classify any deficiency. For example, if written policies do not at least have the categories of policies laid out in the FCPA Guidance "Ten Hallmarks of an Effective Compliance Program"—which states "the nature and extent of transactions with foreign governments, including payments to foreign officials; use of third parties; gifts, travel, and entertainment expenses; charitable and political donations; and facilitating and expediting payments;" and these concepts are also formulated in the Illustrative Guide—such a finding would preclude management from "concluding that the entity has met the requirements for effective internal controls in accordance with the framework."

If, however, there are no objective criteria as laid out in the FCPA Guidance to evaluate your company's compliance internal controls, what steps should compliance officers take?

The Illustrative Guide says that a business' senior management, with appropriate board oversight, "may establish objective criteria for evaluating internal control deficiencies and for how deficiencies should be reported to those responsible for achieving those objectives." Together with appropriate auditing boundaries set by either established law, regulation or standard, or through management exercising its judgment, you can then make a full determination of "whether each of the components and relevant principles is present and functioning and components are operating together, and ultimately in concluding on the effectiveness of the entity's system of internal control."

This means if you fail to implement a control around a high-risk scenario such as gifts, travel, and entertainment; or fail to have effect controls around this area; that would be a major deficiency. Yet if you only lack an internal control or have an ineffective segregation of duties around review of such expenditures, it could be remedied.

The Illustrative Guide has a useful set of templates that can serve as the basis for your reporting results. They are specifically designed to "support an assessment of the effectiveness of a system of internal control and help document such an assessment." The Document, Document, and Document feature is critical in any *best practices* anti-corruption or anti-bribery compliance program, whether based upon the FCPA, U.K. Bribery Act, or some other regulation.

With the Illustrative Guide, COSO has given the compliance practitioner a useful road map to begin an analysis into your company's internal compliance controls. When the SEC comes knocking at your door, this is precisely the type of evidence it will want to see to evaluate whether your company has met its obligations under the FCPA's internal controls provisions.

If you fail to implement a control around a high-risk scenario such as gifts, travel and entertainment, or fail to have effect controls around

First are some general definitions that you need to consider in your evaluation. A compliance internal control must be both present and functioning. A control is present if the "components and relevant principles exist in the design and implementation of the system of [compliance] internal control to achieve the specified objective." A compliance internal control is functioning if the "components and relevant principles continue to exist in the conduct of the system of [compliance] internal controls to achieve specified objectives." In other words, do the controls tie to your company's doing compliance, or are they simply there to have a check-the-box system?

I. Control Environment

Under the objective of Control Environment there are five principles that you will need to assess. They are:

- Principle 1: "The organization demonstrates a commitment to integrity and ethical values." Identify if there is a training program to help make employees cognizant of the importance of doing business ethically and in compliance with the standard's of your company's Code of Conduct. Also, is there specific training on the FCPA, Bribery Act or other relevant anti-corruption legislation that may govern your organization? Next does your company have any process in place to evaluate "individuals against published integrity and ethics policy?"

  Finally, do you have in place any process to "identify and address deviations in the organization?"

- Principle 2: "The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control." Under this principle you must *document* the active involvement of your company's board of directors. So not only must risk assessments be performed and evaluated by senior management; they must also be evaluated by the board—separate and apart from senior management. A board must also document its review of any remediation plans and monitoring activities for your compliance program going forward.

- Principle 3: "Management establishes, with board oversight, [the] structures, reporting lines, and appropriate authorities and responsibility in pursuit of the objectives." You will need to consider not only the structure of your business, but also whether both clear and sufficient reporting lines have been established throughout the company. The next analysis is to move down the chain to see if there definitions and assignments for your compliance function. Lastly, you need to assess whether there are sufficient parameters around the responsibilities of the compliance function and if there are limitations that should be addressed.

- Principle 4: "The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with the objectives." Under this principle you will need to review the policies and procedures to make sure you have the minimum required under a *best practices* compliance program and then evaluate and address any shortcomings. Also, this principle has a more personnel focus by requiring you to consider whether your organization

Do the controls tie to your company's doing compliance, or are they simply there to have a check-the-box system?

attracts, develops, and retains sufficient compliance personnel and whether an appropriate succession plan has been implemented.

- Principle 5: "The organization holds individuals accountable for their internal control responsibilities in the pursuit of the objective." Here, determine whether the board established and communicated the mechanisms to hold employees accountable for your compliance internal controls. As suggested in the FCPA Guidance, there should be both a carrot and a stick approach. This means, for the carrot, you should identify if there is some board, senior management or employee compensation based on whether they did their assignments in compliance with your Code of Conduct—or are bonuses based strictly on a sales formulation? For the stick, have any employees ever been disciplined for violating your compliance regimes?

II. Risk Assessment

This objective has four principles that require assessment. They are:

- Principle 6: "The organization specifies objectives with sufficient clarity to enable the identification and assessmentof risks relating to objectives that include operations, external financial reporting, external non-financial reporting, internal reporting, and compliance objectives." I think the key is the documentation of several different topics and issues relating to your company and how it operates. This means you will need to assess such diverse concepts as what your senior management's choices are for business and compliance. You will need to consider and assess tolerances for risk as demonstrated by issues such as operations and financial performance goals. Finally, it can be used as a basis for committing compliance resources going forward.

- Principle 7: "The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed." This principle requires you to take a look at not only your compliance organization, but also your business structure including entity, subsidiary, division, operating unit, and functional levels. You should assess the involvement of your compliance function at each point identified and the appropriate levels of management therein. Finally, from the compliance perspective, you should attempt to estimate not only the significance of compliance risks identified in risk assessment, but also determine how to respond to such identified compliance risks.

- Principle 8: "The organization considers the potential for fraud in assessing risks to the achievement of objectives. Bribery and corruption can be categorized as forms of fraud." Rather than fraud against the company to obtain personal benefits, the issue here can be fraud in the form of bribery and corruption of foreign government officials. For the compliance internal control assessment around this principle, I would urge you to "follow the money" in your organization and consider the mechanisms

by which employees can generate the funds sufficient to pay bribes. Many of these are simply fraud schemes, so you should consider this within the compliance context and assess incentive and pressures on employees to make their numbers or be fired. You should also assess your employees' attitudes and rationalizations regarding corruption.

- Principle 9: "The organization identifies and assesses changes that could significantly impact the system of internal control." This principle speaks to your organization's need to maintain commitment to use the risk assessment going forward. It also requires you to assess changes in the external environment and in the business model, or other significant business changes and, finally, to consider any changes in compliance leadership and how that would affect this principle.

One thing the Illustrated Guide makes clear is the inter-related nature of internal control. Simply because you may have a deficiency in one specific principle, or even if controls are not present around such a principle, that does not automatically mean a company cannot consider its overall internal controls to be effective. For the compliance officer, this is significant because you may have one principle present but function in the context of another. An example from the Illustrated Guide is the situation where Principle 8, Assessing Fraud Risk, is not present—but if other principles, such as Principle 3, Establishing Structure, Authority and Responsibility, and Principle 5, Enforcing Accountability, adequately address the issue from a control perspective, then the deficiency in Principle 8 is handled.

At the end of the day, unless a major deficiency is noted, it is up to senior management to assess the "severity of an internal control deficiency or combination of deficiencies, in determining whether components and relevant principles are present and functioning, and the components are operating together, and ultimately in determining the effectiveness of the entity's system of internal control." This would also be true from the compliance internal control perspective.

III. Control Activities

Under the component of Control Activities there are three principles that you will need to assess. They are:

- Principle 10: "The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels." Your entity must demonstrate that it integrates its compliance function around its risk assessment. You must demonstrate more than simply an out-of-the-box compliance solution, and that your company has considered specific factors as part of your compliance program, including its relevant business processes, an evaluation of a mix of control activity types, and consideration of at what level such compliance controls are applied. Finally, there must be evidence that your company has addressed segregation of duties from the compliance perspective.

- Principle 11: "The organization selects and develops general control activities over technology to support the achievement of the objectives." A company must determine the dependency between the use of technology in business process and general technology controls. Then there must be evidence that the company has established relevant acquisition, development, and maintenance control activities over said technology. Also, you should have evidence of the establishment of relevant technology infrastructure control activities and relevant security management process control activities.

> Even if controls are not present around such a principle, that does not automatically mean a company cannot consider its overall internal controls to be effective

- Principle 12: "The organization deploys control activities through policies that establish what is expected and procedures to put policies into action." This principle means management should put sufficient compliance policies and procedures in place to support the company's anti-corruption compliance mandates, and require training of employees on these compliance policies and procedures (with testing to determine the adequacy of such compliance training). It also requires evidence that sufficient incentives have been implemented for employees to follow the compliance regime, with a timely discipline process for those employees who fail to comply. Finally, it requires evidence of constant re-assessments of the policies and procedures.

IV. Information and Communication

This objective has three principles that require assessment. They are:

- Principle 13: "The organization obtains (or generates) and uses relevant, quality information to support the functioning of internal control." This means that you must identify information requirements for your compliance program and then capture that data via internal and external sources. If you cannot do so, you must explain why. You must process the information and use it in your compliance function going forward and document it as well.

- Principle 14: "The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control." Under this principle you must be able to demonstrate that your company communicates compliance internal control information with not only senior management, but also appropriate employees and your board of directors. It re-emphasizes the need for separate lines of communications and documented consideration to show why you selected the relevant methods of communication.

- Principle 15: "The organization communicates with external parties regarding matters

affecting the functioning of internal control." This principle relates to your communications to third parties, so you will need to demonstrate internal controls around your compliance communications with parties external to your company. You will also be required to show compliance internal controls inbound to your organization from third parties.

V. Monitoring Activities

The Monitoring Activities objective consists of two principles that require assessment. They are:

- Principle 16: "Organization selects, develops and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning." This requires that you to have employees knowledgeable in your business processes who can review them on an ongoing basis. You must show that compliance internal controls exist that objectively evaluate the rates of compliance change, with an understanding of the baseline and projected business changes. All of this must be integrated with business processes with appropriate adjustments in scope and frequency.

Management should put sufficient compliance policies and procedures in place to support the company's anti-corruption compliance mandates

- Principle 17: "The organization evaluates and communicates internal control deficiencies timely to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate." Under this principle, you must be able to demonstrate that from the compliance perspective, your results were assessed, any deficiencies were communicated to the appropriate parties, and finally, any appropriate corrective action was taken.

I regularly say that the three most important words for FCPA compliance are document, document, and document. I believe the COSO 2013 Framework puts that point into perspective, particularly with the auditing requirement. As noted by Ron Kral, you must: "Verify the adequacy of your documentation and alignment of controls to the 17 principles with the external auditors at key junctions and decision points. Also, consider involving your internal audit function in answering this question. Not only do you want assurance that your documentation of control design is adequately aligned, but also that the controls are operating

The three most important words for FCPA compliance are document, document, and document

effectively."

The SEC enforcement action against BHP Billiton in May 2015 makes clear that internal controls must be effective to pass muster under the books-and-records provisions of the FCPA, and that effectiveness must be demonstrable. In that case, BHP Billiton had a robust set of internal controls around its hospitality program from the 2008 Olympics—yet the company did not follow its own internal controls. By failing to do so, BHP rendered those controls ineffective. Moreover, as internal controls arguably have a strict liability standard, if you cannot document the effectiveness of your internal controls, your company may be in violation of the FCPA simply for that transgression—regardless of whether any actual bribery did or did not happen.

The auditing process should work to determine not only if your compliance internal controls are properly designed and operating effectively, but also that the five components of the COSO framework are operating together. Kral believes that this is critical for any sound internal control evaluation. "It's not merely a matter of satisfying documentation and compliance requirements, but rather a matter of protecting the interests of shareholders," he writes. I agree. By going through the auditing exercise, you will have created a framework to operate, assess, and update your compliance internal controls to meet the ever-changing nature of FCPA (and other anti-corruption) compliance programs.

Good compliance is simply good business. These COSO objectives are not only important from the compliance perspective; they also speak to the issue of overall process in your organization. The more you can burn these activities into the DNA of your company, the smoother your organization will run going forward. Auditing against the COSO standards will provide your management with greater information on the health of your organization and satisfy your legal requirements under the FCPA.