HALLMARK II

Code of Conduct, Policies and Procedures & Internal Controls

Thomas Fox

The Compliance Evangelist

A. The Code of Conduct

What is the value of having a Code of Conduct? I have heard many business folks ask that question over the years. In its early days, a Code of Conduct tended to be lawyer-written and lawyer-driven to wave in regulator's face during an enforcement action by using it to claim we are an ethical company. Is such a legalistic code effective? Is a Code of Conduct more than simply, your company's law? What should be the goal in the creation of your company's Code of Conduct?

In the 2012 FCPA Guidance, the DOJ and Securities and Exchange Commission stated, "A company's code of conduct is often the foundation upon which an effective compliance program is built. As DOJ has repeatedly noted the most effective codes are clear, concise, and accessible to all employees and to those conducting business on the company's behalf." Indeed, it would be difficult to effectively implement a compliance program if it was not available in the local language so that employees in foreign subsidiaries can access and understand it. When assessing a compliance program, DOJ and SEC will review whether the company has taken steps to make certain that the code of conduct remains current and effective and whether a company has periodically reviewed and updated its code."

In the Society for Corporate Compliance and Ethics (SCCE) 2017 Complete Compliance and Ethics Manual, article, entitled "*Essential Elements of an Effective Ethics and Compliance Program*", authors Debbie Troklus, Greg Warner and Emma Wollschlager Schwartz, state that your company's Code of Conduct "First and foremost, the standards of conduct demonstrate the organization's overarching ethical attitude and its "system-wide" emphasis on compliance and ethics with all applicable laws and regulations." They go on to state, "The code is meant for all employees and all representatives of the organization, not just those most actively involved in known compliance and ethics issues. This includes management, vendors, suppliers, and independent contractors, which are frequently overlooked groups." From the board of directors to volunteers, the authors believe that "everyone must receive, read, understand, and agree to abide by the standards of the Code of Conduct."

There are several purposes which should be communicated in your Code of Conduct. The overriding goal is for all employees to follow what is required of them under the Code of Conduct. You can do this by communicating those requirements, to providing a process for proper decision-making and then requiring that all persons subject to the Code of Conduct put these standards into everyday business practice. Such actions are some of your best evidence that your company "upholds and supports proper compliance conduct."

The substance of your Code of Conduct should be tailored to your company's culture, and to its industry and corporate identity. It should provide a mechanism by which employees who are trying to do the right thing in the compliance and business ethics arena can do so. The Code of Conduct can be used as a basis for employee review and evaluation. It should certainly be invoked if there is a violation. Your company's disciplinary procedures be stated in the Code of Conduct. These would include all forms of disciplines, up to and including dismissal, for serious violations of the Code of Conduct. Further, your company's Code of Conduct should emphasize it will comply with all applicable laws and regulations, wherever it does business. The Code needs to be written in

plain English and translated into other languages as necessary so that all applicable persons can understand it.

As I often say, the three most important things about your compliance program are 'Document, Document and Document'. The same is true in communicating your company's Code of Conduct. You need to do more than simply put it on your website and tell folks it is there, available and that they should read it. You need to document that all employees, or anyone else that your Code of Conduct is applicable to, has received, read, and understands it. The DOJ expects each company to begin its compliance program with a very public announced, very robust Code of Conduct. If your company does not have one, you need to implement one forthwith. If your company has not reviewed or assessed your Code of Conduct for five years, I would suggest that you do in short order as much has changed in the compliance world.

How important is the Code of Conduct? Consider the 2016 SEC enforcement action involving United Airlines, which turned on violation of the company's Code of Conduct. The breach of the Code of Conduct was determined to be a FCPA internal controls violation. It involved a clear quid pro quo benefit paid out by United Airlines to David Samson, the former Chairman of the Board of Directors of the Port Authority of New York and New Jersey, the public government entity which has authority over, among other things, United Airlines operations at the company's huge east coast hub at Newark, NJ.

The actions of United's former Chief Executive Officer, Jeff Smisek, in personally approving the benefit granted to favor Samson violated the company's internal controls around gifts to government officials by failing to not only follow the United Code of Conduct but also violating it. The $2.4 million civil penalty levied on United was in addition to the Non-Prosecution Agreement settlement with the Department of Justice, which resulted in a penalty of $2.25 million. The scandal also cost the resignation of Smisek and two high-level executives from United.

Three Key Takeaways

1. Every formulation of a best practices compliance program starts with a written Code of Conduct.
2. The substance of your Code of Conduct should be tailored to the company's culture, and to its industry and corporate identity.
3. Document Document Documents your training and communication efforts.

B. Policies and Procedures

There are numerous reasons to put some serious work into your compliance policies and procedures. They are certainly a first line of defense when the government comes knocking. The 2012 FCPA Guidance made clear that "Whether a company has policies and procedures that outline responsibilities for compliance within the company, detail proper internal controls, auditing practices, and documentation policies, and set forth disciplinary procedures *will also be considered by DOJ and SEC*." And by using the word "considered", it is clear that this means the regulators will take a strong view against a company that does not have well thought out and articulated set of policies and procedures; all of which are systematically reviewed and updated. Moreover, having policies written out and signed by employees provides what some consider the most vital

layer of communication and acts as an internal control. Together with a signed acknowledgement, these documents can serve as evidentiary support if a future issue arises. In other words, the 'Document, Document and Document' mantra applies just as strongly to this area of anti-corruption compliance.

The specific written policies and procedures required for a *best practices* compliance program are well known and long established. The 2012 FCPA Guidance stated, "Among the risks that a company may need to address include 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." Policies help form the basis of expectation for conduct in your company. Procedures are the documents that implement these standards of conduct.

The role of compliance policies is to protect companies, their stakeholders, including employees, third-parties and others, despite an occasional lapse. A company's compliance policies provide a basic set of guidelines for employees and others to follow. Compliance policies should give general prescriptions and should be supplemented by more specific procedures. By establishing what is and what is not acceptable ethical and compliant behavior, a company helps mitigate the risks posed by employees who might not always make the right ethical choices.

The Evaluation of Corporate Compliance Programs builds up on the requirements articulated in the 2012 FCPA Guidance. Under Prong 4, Policies and Procedures, there are two parts: Design and Accessibility and Operational Integration. This Part A has the following components.

Designing Compliance Policies and Procedures – *What has been the company's process for designing and implementing new policies and procedures? Who has been involved in the design of policies and procedures? Have business units/divisions been consulted prior to rolling them out?*

Applicable Policies and Procedures – *Has the company had policies and procedures that prohibited the misconduct? How has the company assessed whether these policies and procedures have been effectively implemented? How have the functions that had ownership of these policies and procedures been held accountable for supervisory oversight?* The Evaluation then goes on to ask about both accessibility and effectiveness of the compliance policies and procedures by stating,

Accessibility – *How has the company communicated the policies and procedures relevant to the misconduct to relevant employees and third parties? How has the company evaluated the usefulness of these policies and procedures?*

Compliance policies do not guarantee employees will always make the right decision. However, the effective implementation and enforcement of compliance policies demonstrate to the government that a company is operating professionally and ethically for the benefit of its stakeholders, its employees and the community it serves.

There are five general elements to a compliance policy. It should stake out the following:

- identify who the compliance policy applies to;
- set out what is the objective of the compliance policy;

- describe why the compliance policy is required;
- outline examples of both acceptable and unacceptable behavior under the compliance policy; and
- lay out the specific consequences for failure to comply with the compliance policy.

The Evaluation mandates there must be communication of your compliance policies and procedures throughout the workforce and relevant stakeholders such as third-parties and business venture partners. Under Part B of Prong 4 is the Operational Integration section with the following components.

Responsibility for Integration – *Who has been responsible for integrating policies and procedures? With whom have they consulted (e.g., officers, business segments)? How have they been rolled out (e.g., do compliance personnel assess whether employees understand the policies)?*

There are also two specific area that policies and procedures need to focus on. They are around payments and third parties. They have the following components.

Payment Systems – *How was the misconduct in question funded (e.g., purchase orders, employee reimbursements, discounts, petty cash)? What processes could have prevented or detected improper access to these funds? Have those processes been improved?*

Vendor Management – *If vendors had been involved in the misconduct, what was the process for vendor selection and did the vendor in question go through that process?*

This means that it more than simply having appropriate policies and procedures. It is operationalizing them into your compliance program, down to the business unit level. How can you do so? Compliance training is only one type of communication. This is a key element for compliance practitioners because if you have a 30,000+ worldwide work force, simply the logistics of training can appear daunting. Small groups, where detailed questions about policies can be raised and discussed, can be a powerful teaching tool. Another technique can be the posting FAQ's in common areas and virtually. Also, having written compliance policies signed by employees provides what some consider the most vital layer of communication. A signed acknowledgement can serve as evidentiary support if a future issue arises. Finally, never forget the example of the Morgan Stanley declination where the recalcitrant employee annually signed such certifications. These signed certifications help Morgan Stanley walk away with a full declination.

The 2012 FCPA Guidance ends its section on policies with the following, "Regardless of the specific policies and procedures implemented, these standards should apply to personnel at all levels of the company." It is important that compliance policies and procedure are applied fairly and consistently across the organization. The Fair Process Doctrine demonstrates that if compliance policies and procedures are not applied consistently, there is a greater chance that an employee dismissed for breaching a policy could successfully claim he or she was unfairly terminated. This last point cannot be over-emphasized. If an employee is going to be terminated for fudging their expense accounts in Brazil, you had best make sure that same conduct lands your top producer in the US with the same quality of discipline.

Three Key Takeaways

1. The Code of Conduct, together with written compliance policies and procedures form the backbone of your compliance program.
2. The DOJ and SEC expect a well-thought out and articulated set of compliance policies and procedures.
3. The Fair Process Doctrine holds for the application of policies and procedures.

C. Internal Controls and Compliance

What specifically are internal controls in a compliance program? Internal controls are not only the foundation of a company but are also the foundation of any effective anti-corruption compliance program. The starting point is the FCPA itself, 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—
(i) transactions are executed in accordance with management's general or specific authorization;
(ii) 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;
(iii) access to assets is permitted only in accordance with management's general or specific authorization; and
(iv) the recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any
differences ….

The DOJ and SEC, in the 2012 FCPA Guidance, stated, "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."

This was supplemented in the Evaluation of Corporate Compliance Programs with the following:
Controls – *What controls failed or were absent that would have detected or prevented the misconduct? Are they there now?*

Aaron Murphy, Assistant Solicitor General in the Office of the Attorney General for the state of Utah and author of "*Foreign Corrupt Practices Act: A Practical Resource for Managers and Executives*", said, "Internal controls are 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 Joe Howell, EVP at Workiva, Inc. has said that internal controls are systematic measures, such as reviews, checks and balances, methods and procedures, instituted by an organization that performs several different functions. These functions include allowing a company to conduct its business in an orderly and efficient manner; to safeguard its assets and resources, to detect and deter errors, fraud, and theft; to assist an organization ensuring the accuracy and completeness of its accounting data; to enable a business to produce reliable and timely financial and management information; and to help an entity to ensure there is adherence to its policies and plans by its employees, applicable third parties and others. Howell adds that internal controls are entity wide; that is, they are not just limited to the accountants and auditors. Howell also notes that for compliance purposes, controls are those measures specifically 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 as well as the distribution of assets.

Why are internal controls important in your compliance program? Several FCPA enforcement actions demonstrate the reasons. The first was the criminal plea obtained by DOJ from Weatherford International. There were three areas where the company failed to institute appropriate internal controls. First, around third parties and business transactions, limits of authority and documentation requirements. Second, on effectively evaluating business transactions, including acquisitions and joint ventures, for corruption risks and to investigate those risks when detected. Finally, around 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 involved the gun manufacturer Smith & Wesson. The case was a civil matter was prosecuted administratively by the SEC. In its Administrative Order, the SEC stated, "Smith & Wesson failed to devise and maintain sufficient internal controls with respect to its 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".

The third example is circumvention of existing internal controls with no justification or appropriate compliance function oversight. It comes from the SEC enforcement action against Halliburton for

hiring an Angolan agent by moving him from commercial agent status to that of a supplier so the approval process would be easier. However, the internal controls process around using a supplier also had rigor as it required a competitive bidding process which would take several months to complete. Over-riding this internal control, the local business team was able to contract with the Angolan agent for these services, all without the Angolan agent going through the procurement internal controls.

A second internal control which was over-ridden was the procurement requirement that the supplier procurement process begin with "an assessment of the critically or risk of a material or services"; not with a particular supplier and certainly not without "competitive bids or providing an adequate single source justification." There was a separate internal control that required "contracts over $10,000 in countries with a high risk of corruption, such as Angola, to be reviewed and approved by a Tender Review Committee." This internal control was also over-ridden.

Halliburton internal controls required that when a single source was used by the company it had to be business justification. This justification would require a showing of preference for quality, technical, execution or other reasons, none of which were demonstrated by the Angolan agent. Finally, if such a single source was used, the reasons had to be documented or in Halliburton's internal controls language "identified and justified". None were documented by the company.

Finally, as the internal controls were either circumvented or over-ridden; "As a consequence, internal audit was kept in the dark about the transactions and its late 2010 yearly review did not examine them." This was yet another internal control failure but was built on the previous failures noted above.

The whole concept of internal controls is that companies need to focus on where the risks are, whether they be compliance risks or other, and they need to allocate their limited resources to putting controls in place that address those risks, and in the compliance world, of course, your two big risks are the assets or resources of a company. Not just cash but inventory, fixed assets etc., being used to pay a bribe, and then the second big element would be diversion of company assets, such as unauthorized sales discounts or receivables and write offs, which are used to pay a bribe.

There are four significant controls that I would suggest the compliance practitioner implement initially. They are: (1) Delegation of Authority (DOA); (2) Maintenance of the vendor master file; (3) Contracts with third parties; and (4) Movement of cash / currency.

Your DOA should reflect the impact of compliance risk including both transactions and geographic location so that a higher level of approval for matters involving third parties, for fund transfers and invoice payments to countries outside the US would be required inside your company.

Next is the vendor master file, which 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. There should be electronic controls in place to block payments to any vendor for which

vetting has not been approved. Internal controls are needed over the submission, approval, and input of changes to the vendor master file.

Contracts with third parties can be a very effective internal control which works to prevent nefarious conduct rather than simply as a detect control. I would caution that for contracts to provide effective internal controls, relevant terms of those contracts, including for instance the commission rate, reimbursement of business expenses, use of subagents, etc.,) should be made available to those who process and approve vendor invoices.

All situations involving the movement of cash or transfer of monies outside the US, including such methods AP computer checks, manual checks, wire transfers, replenishment of petty cash, loans, advances; should all be reviewed from the compliance risk standpoint. This means you need to identify the ways in which a country manager or a sales manager, could cause funds to be transferred to their control and to conceal the true nature of the use of the funds within the accounting system.

To prevent these types of activities, internal controls need to be in place. All wire transfers outside the US should have defined approvals in the DOA, and the persons who execute the wire transfers should be required to evidence agreement of the approvals to the DOA and wire transfer requests going out of the US should always require dual approvals. Lastly, wire transfer requests going outside the US should be required to include a description of proper business purpose.

The bottom line is that internal controls are just good financial controls. The internal controls that detailed for third party representatives in the compliance context will help to detect fraud, which could well lead to bribery and corruption. As an exercise, I suggest that you map your existing internal controls to the Ten Hallmarks of an Effective Compliance Program or some other well-known anti-corruption regime to see where control gaps may exist at your organization. This will help you to determine whether adequate compliance internal controls are present in your company. From there you can move to see if they are working in practice or 'functioning'.

Three Key Takeaways

1. Effective internal controls are required under the FCPA.
2. Internal controls are a critical part of any best practices compliance program.
3. The Weatherford, Smith & Wesson, and Halliburton SEC, FCPA enforcement actions demonstrate the enforcement spotlight on internal controls.