The FCPA REPORT

www.fcpareport.com Volume 4, Number 25 December 2, 2015

# COMPLIANCE POLICIES AND PROCEDURES

## Defining, Documenting and Measuring Compliance Program Effectiveness

By Vincent Pitaro

The risks of having a compliance program that exists only on paper are well-known, but measuring whether the program is actually working, how it is working, and documenting those findings for internal and external stakeholders present challenges. A recent program at the SCCE Annual Compliance & Ethics Institute considered how compliance professionals can take steps, through documentation and measurement, to demonstrate the effectiveness of their compliance programs. The program featured Scott Hilsen, a managing director at KPMG Forensic and Jean-Paul Durand, a vice president and chief ethics and compliance officer at Tech Data Corporation. See also "*How Can CCOs Demonstrate Compliance Program Effectiveness*?," The FCPA Report, Vol. 3, No. 19 (Sep. 24, 2014).

According to Hilsen, external stakeholders, such as investors, lenders and regulators, want to know that a company's compliance program can prevent and detect misconduct and that it is attempting in good faith to assure compliant behavior. Internal stakeholders want to know that the compliance program protects the company, uses resources effectively and is governed by a reliable process. Demonstrating that a compliance program is effective involves three steps, said Hilsen: defining effectiveness, documenting compliance and measuring compliance.

### *1) Defining Effectiveness*

Effectiveness can mean different things to different stakeholders. Hilsen suggested a few possible metrics:

- Does it reduce misconduct or violations?
- Is it on budget?
- Does it identify and resolve issues in a timely manner?
- Does it identify program shortcomings and risks and mitigate those risks?
- Are employees and business partners being trained?

Compliance professionals must first decide what they want to measure and why, he said. Second, they should set achievable goals. Finally, they should seek buy-in from all stakeholders. Durand noted that some companies consider avoiding fines and employee reports of misconduct signs of effectiveness. These may create a false sense of security because they could also indicate that a company does not understand where its true risks lie. In Hilsen's experience, regulators typically ask three questions about compliance programs, which can be used as a framework for measuring compliance effectiveness:

- Is the program well-designed? This concerns policies, procedures, oversight, the number of compliance professionals and their skills, as well as the resources devoted to the program. See, e.g., "*In-House Compliance Experts Share Five Strategies for Building a High-Performing Compliance Team*," The FCPA Report, Vol. 4, No. 23 (Nov. 4, 2015).
- Is it applied in good faith? Regulators expect a company to be actively training employees, communicating with business partners, assuring that the compliance message is getting across, and adapting to changing business circumstances. See "*Six Steps for Converting a 'Paper' FCPA Compliance Program into a Pervasive Culture of Anti-Bribery Compliance (Part One of Two)*," The FCPA Report, Vol. 2, No. 4 (Feb. 20, 2013); Part Two, Vol. 2, No. 5 (Mar. 6, 2013).

©2015 The FCPA Report. All rights reserved.

- Does it work? Policy violations do not mean that a program is not working. Regulators are concerned with whether violations are detected, investigated and remediated.

### *2) Documenting Compliance*

Documentation is essential for demonstrating to stakeholders that a program is effective, Hilsen explained. It should show that the company knows what it is measuring and how.

When documenting, companies should focus on perceived gaps in their compliance framework, said Durand. In doing so, it can be helpful to measure a program against a known framework, such as the SEC-DOJ FCPA Resource Guide or the Committee of Sponsoring Organizations of the Treadway Commission (COSO) internal controls framework.

Regulators do not expect "absolute perfection," he said. Rather, they expect "continual improvement," including efforts to address perceived gaps in a program. Regulators expect to see specified goals and documentation that the company is working towards those goals, said Hilsen. He added that it is not necessary for a company to have all documentation in one place, but it must know where it is, and it must be readily accessible. Durand reiterated the now-common SEC observation that if something is not documented, "it didn't happen." The panelists discussed the following specific areas of compliance that should be properly documented.

#### *Governance and Oversight*

Even if a company's dedicated compliance function is small, other stakeholders within an organization, such as human resources or regulatory compliance personnel, may have their own interests in compliance, which can support the compliance function, Durand explained. An organizational chart can be used to aggregate that information and identify all of the stakeholders throughout the organization that are involved in compliance. Job descriptions, which specify individuals' responsibilities, are an even more basic source of information. A document that describes management's role in ethics and compliance is also a critical tool.

Another important element, Durand said, is understanding and documenting the board's role in compliance – how it is structured, what its responsibilities are, and what it expects of compliance professionals. See "*Anti-Corruption Compliance Best Practices for Boards of Directors,*" The FCPA Report, Vol. 2, No. 12 (Jun. 12, 2013). Board minutes can be a source of compliance-related information. It is important, Hilsen added, to assure that the compliance efforts of external stakeholders, such as subsidiaries and joint venture partners, are also properly documented.

#### *Policies, Procedures and Controls*

A company should be ready to show regulators thoroughly documented compliance policies, processes and procedures, and internal controls, said Hilsen. See, e.g., "*$9.5 Million SEC FLIR Settlement Emphasizes Benefits of Self-Reporting and Importance of Internal Controls,*" The FCPA Report, Vol. 4, No. 8 (Apr. 15, 2015). Because not all compliance functions are centralized, the compliance professionals must be vigilant about documenting changes to the compliance program. For example, compliance-related contract provisions may change over time or by region, so it is not enough simply to know what contracts are outstanding, Hilsen said. Durand recommended that, in order to keep track of such information and changes, compliance professionals should be involved with business people as new business is developed.

#### *Risk Assessments*

One of the first things regulators ask, said Hilsen, is whether a company has conducted a risk assessment. Durand explained that a company should document what it is going to measure, how it is going to measure it, who will do the measuring, and how frequently. Risk assessments should "first, do no harm," he said. A company may be worse off if it identifies a risk and fails to do anything about it. It must follow through

©2015 The FCPA Report. All rights reserved.

and implement remedial processes. He noted that an organization has a great deal of flexibility in determining how to address risks and build a risk assessment process. See "*Mitigating Bribery Risks Using Financial Controls, Risk Assessments and Leveraging Internal Resources*," The FCPA Report, Vol. 3, No. 18 (Sep. 10, 2014).

### *Training and Communication*

According to Hilsen, a company must keep attendance lists and track the various iterations of its training materials. The Morgan Stanley declination showed that proof of frequent compliance training is very powerful and persuasive evidence. Durand cautioned, however, that companies should be careful about "training fatigue" and training employees on things they do not need to know. Training should be tailored to employees' specific circumstances, he recommended. See "*NAVEX Global Identifies Key Hurdles to Effective Compliance Training and Offers Tips to Overcome Them*," The FCPA Report, Vol. 4, No. 18 (Sep. 9, 2015).

### *Hotlines*

Some firms employ full-time ethics advisers who are available to answer employees' questions about ethics and compliance, Durand said. He noted that there is a great deal of information available on the types and frequency of reports that businesses receive through hotlines. A company can use such data to see how it compares to its peers. See "*Companies Seeing an Increase in Hotline Reports and Higher Numbers of Repeat Reporters*," The FCPA Report, Vol. 4, No. 8 (Apr. 15, 2015); and "*How Does Your Company's Anti-Corruption Hotline Compare?*," The FCPA Report, Vol. 3, No. 21 (Oct. 22, 2014). Hilsen added that, not only should a company document its hotline reports, but it should also document the process by which it handles and responds to such reports.

Durand observed that it is important to record and respond appropriately to each hotline report, following a predetermined process, even with respect to minor matters. See our Q&A series on anti-corruption hotlines: "*Interview with Janice Innis-Thompson, Senior Vice President and Chief Compliance Officer at TIAA-CREF*," The FCPA Report, Vol. 4, No. 1 (Jan. 7, 2015); "Interview with Benjamin Haley of Covington & Burling," Vol. 3, No. 19 (Sep. 24, 2014); and "Interview with Brandon Daniels, President of Managed Services, Clutch Group," Vol. 3, No. 24 (Dec. 3, 2014).

### *Auditing and Monitoring*

Third-party reviews and monitoring are essential to assure the effectiveness of a compliance program, said Hilsen. See "*In-House and Outside Counsel Share Advice on Risk Assessments, Gift Policies and Third-Party Due Diligence*," The FCPA Report, Vol. 4, No. 12 (Jun. 10, 2015). A firm should maintain a schedule of when it will conduct third-party due diligence and risk assessments and document how it will respond to those risk assessments. He noted that the information needed to document program effectiveness may reside with other internal stakeholders. For example, many internal controls are compliance controls, which may be monitored by the internal audit function. See "*How Companies Can Use Enhanced Auditing Techniques to Address the Government's Increasing Focus on Internal Controls*," The FCPA Report, Vol. 4, No. 10 (May 13, 2015). Durand added that data analytics can be used to identify issues and demonstrate a compliance program's effectiveness.

### *Investigations*

An internal investigation process may be decentralized, drawing from different functions within the business, or centralized in one area, Durand said. It is important to document the process for conducting an investigation, especially when the process is decentralized. The process should include templates for matters such as case planning, case reporting and interview techniques – and relevant personnel should be trained on how to follow that process. Each investigation and its outcome should be documented. See, e.g., "*How to Conduct an Anti-Corruption Investigation: Ten Factors to Consider at the Outset (Part One of Two)*," The FCPA Report, Vol. 2, No. 25 (Dec. 18, 2013); Part Two, Vol. 3, No. 1 (Jan. 8, 2014).

©2015 The FCPA Report. All rights reserved.

### *Enforcement*

Accountability, said Hilsen, is critical to showing that a compliance program is effective. Regardless of whether a firm has formal disciplinary procedures, or deals with discipline on an ad hoc basis, he said, it must document that "people are being held accountable" and that discipline is meted out fairly and effectively. A violation of policies and procedures should have consequences for the responsible party and senior personnel should be subject to the same sanctions as other employees. Durand added that demonstrating appropriate discipline to regulators may be the most important factor in an examination. If a company cannot show that people are held accountable, the rest of the documentation about the compliance program may not have much impact. See "*When, Why and How Should Companies Discipline Employees for FCPA Violations?*," The FCPA Report, Vol. 1, No. 8 (Sep. 19, 2012).

### *Remediation*

Hilsen said that, not only must a company identify weaknesses in its compliance program and propose policy changes, but it must also make sure that it effectively implements those recommendations. It should document that it identified a risk or weakness, made recommendations to address it, set a time frame for doing so, and completed the process, thereby eliminating the risk. There is no better evidence of an effective compliance program than well-documented risks and associated remedial efforts, he added. See "*Best Practices for Reviewing Anti-Corruption Compliance Programs: Implementation, Remediation and Documentation (Part Three of Three)*," The FCPA Report, Vol. 2, No. 18 (Sep. 11, 2013).

### *Privilege*

Many elements of compliance programs are not protected by the attorney-client privilege, Hilsen explained. Non-privileged matters include facts, risks, control gaps and remedial activities. On the other hand, advice and conclusions drawn from consultations with in-house counsel are generally privileged. He urged companies to be cautious about claiming privilege, because regulators do not like to hear that a company has conducted a risk assessment, but that it is privileged. Durand noted that it is possible to take a nuanced approach to privilege. For example, the data from a risk assessment may not be privileged, but the company's analysis of the data might. There is a balance between claims of privilege and transparency with regulators. See, e.g., "*D.C. Circuit Confirms Applicability of Attorney-Client Privilege to Internal Investigations*," The FCPA Report, Vol. 3, No. 16 (Aug. 6, 2014); and "*Three Questions to Ask After Detecting a Possible FCPA Violation*," The FCPA Report, Vol. 3, No. 11 (May 28, 2014).

## *3) Measuring Compliance*

Measuring compliance, said Hilsen, involves measuring both activity and effectiveness. Durand said that budgetary and resource constraints, and possible lack of data, can make measurement challenging. Be "creative and thoughtful" about what the company proposes to do and how, he said. A company should use data metrics to assess the effectiveness of its program, but it should also consult with its board of directors to learn their perceptions of the company's culture. Hilsen said that, when trying to measure compliance, a company should ask the same questions as when designing a program:

- Is the program well designed? Consider whether controls are being tested and whether resources are being used appropriately and within budget.
- Is it applied in good faith? Consider the effectiveness of training, auditing, monitoring, discipline and remediation.
- Does it work? Consider employee reporting (through hotlines and other means), employee awareness, and the effectiveness of investigations.

Durand highlighted several types of metrics that can be used to answer those questions. They include whether issues are processed correctly and resolved in a timely manner; the timing and completion of remedial efforts; whether the compliance budget is used effectively; completion of training; and results of various reviews, questionnaires and audits. He cautioned, however,

©2015 The FCPA Report. All rights reserved.

that even if a company has well-documented compliance efforts, it will not pass regulatory muster if the company does not also promote a culture of "transparency and speaking up." Hilsen added that it can be helpful to show that employees and business partners have a good perception of those compliance efforts.

Data to measure those metrics may come from risk assessments, hotline reports, questionnaires, outside reviews and industry benchmarks. Hilsen believes that surveys are underutilized. A survey that asks the right employees the right questions can provide helpful data points and benchmarks for future assessments. There is no substitute for human contact, he said. Getting out and speaking to employees can be an excellent means of obtaining relevant information. Durand added that properly designed exit interviews can be used in the same way. For more on measuring program effectiveness, see "*Guide to Creating an Effective Compliance-Based Employee Incentive Program (Part One of Two)*," The FCPA Report, Vol. 4, No. 1 (Jan. 7, 2015); and "*Strategies for Justifying Compliance and Ethics Budgets*," The FCPA Report, Vol. 3, No. 24 (Dec. 3, 2014).

©2015 The FCPA Report. All rights reserved.