The Development of a Compliance Culture

By

Jeffrey C. Morton
Adviser Compliance Associates, LLC
Morristown, New Jersey
The development of a compliance culture

Jeffrey C. Morton

Abstract

Purpose – To provide the investment management industry with a summary of the expectations of the Securities and Exchange Commission (SEC)'s examination staff with regard to the development of a culture of compliance.

Design/methodology/approach – A review of certain elements identified by an SEC staffer that are necessary for a firm to have a strong and effective control environment and culture of compliance was carried out. The article explores a firm's strategic vision or “tone at the top,” risk identification, establishment of controls, documentation, accountability and self reporting, and cooperation.

Findings – Confirmation that a firm's success in establishing a culture of compliance is difficult to prove and harder to document. However, an understanding of the concept of developing a compliance culture can allow compliance officers to demonstrate a commitment to ethical and compliant practices.

Originality/value – The SEC's new inspection program evaluates each firm's commitment to compliance and moral and ethical practices. This article provides a basic understanding of the minimum expectations of the SEC's inspection staff.

Keywords Corporate governance, Investments

Paper type Technical

It has been exactly three years since the Securities and Exchange Commission (SEC) began vigorously emphasizing the importance of a firm's “culture of compliance”[1] or “moral DNA.”[2] Since April 2003, these phrases have appeared on the SEC's web site (See www.sec.gov) in various speeches and public statements made by SEC officials a total of 54 and 12 times, respectively.

It is not a coincidence that government officials recently intensified their promotion of the concept of companies being moral and ethical. Every day for the first three years of the twenty-first century, you expected to pick up the morning newspaper and read about the next Worldcom, Enron, disgraced research analyst, or market timing scandal. One might argue that Arthur Andersen was not put out of business because of aggressive accounting or the mishandling of Enron-related documents but rather for not maintaining a firm-wide culture of compliance. For the first time in decades, the financial services industry was having a difficult time floating the argument that “a few bad apples were making the industry look bad.” It seemed as though the entire barrel was rotten[3].

With the passage of time and a host of new rules and regulations[4], the wave of corporate scandals, investor lawsuits, and regulatory enforcement actions appears to be subsiding. But the fallout is still with us. We now live in a world where investors and shareholders are focused, at least in part, on the perception of a company's integrity, ethics, and corporate governance values[5]. As Jack Welch, former Chairman and CEO of General Electric said in a 2002 Wall Street Journal Op-Ed piece: “One thing I learned during my years as CEO is that perception matters. And in these times when public confidence and trust have been shaken, I’ve learned the hard way that perception matters more than ever”[6]. This article will explore
the intricate steps involved in developing a corporate culture of compliance and the practical ways to achieve and maintain it.

**Understanding a culture of compliance**

The SEC’s examination staff has indicated that an investment adviser’s risk profile will be correlated to examination frequency and scope[7]. In other words, a firm is likely to be inspected more often and more intrusively if it has not developed a strong firm-wide control environment or “culture of compliance” that highlights a commitment to ethical practices and to serving the best interests of its advisory clients.

In a report prepared by the SEC’s Office of Compliance Inspections and Examinations (OCIE) at the request of Senator Richard C. Shelby, Chairman of the US Senate Committee on Banking, Housing and Urban Affairs, the Staff indicted that in 2003 it changed its examination methodology to:

. . . provide a more formal assessment of firms’ internal compliance and control processes by use of a risk evaluation methodology designed to guide examiners in their evaluation of firms’ risk assessment, mitigation, and management processes. The methodology requires examiners to evaluate the effectiveness of the firm’s controls in each of several key risk areas, and to assess the overall risk and compliance culture of the firm [emphasis added][8].

The difficult thing for most firms to grasp is what it actually means to develop a “culture of compliance.” It is more of a subjective concept than anything else; it is evidenced in the positive feeling an SEC examiner gets when she is completing your firm’s examination. She knows, or at least has a very good gut feeling, that your firm is not going to blow up and be on the front page of the *Wall Street Journal* or *The New York Times* within the next five years. She certainly does not want that to happen on her watch.

Gene Gohlke, Associate Director of the SEC’s OCIE, gave several tangible examples of what it means to create a culture of compliance, including: cooperative attitudes, providing information in a timely manner, availability of senior management (e.g. for opening and closing interviews with regulators), access to memos to employees, internal communication from senior management (e.g. e-mails), consistent disciplinary action (are the stars left to manage themselves?), compliance department funding, and the judicious use of attorney-client privilege[9].

**SEC examination staff approach**

During its inspections, SEC staff will search for documentation to support a firm’s culture of compliance. For most, this is easier said than done. When asked to comment on Wall Street’s need for a Hippocratic Oath or Code of Ethics, investment banker Felix Rohatyn summed it up best: “It’s really something that has to be embedded in an organization all the way up and down. Ultimately, it has to be instinctive”[10]. A culture of compliance or moral DNA is not something that can be purchased off the shelf or taught by a high-priced management consultant. It is something that must be ingrained into the fabric of the firm itself and requires the support of the firm’s most senior management.

The SEC’s examination staff has prepared a formal approach to assessing a firm’s culture of compliance; the staff believes that the following five elements are necessary in order for a firm to have a strong and effective control environment and culture of compliance:

1. strategic vision (also known as compliance goals or objectives);
2. identification of risks;
3. establishment of controls;
4. documentation; and
Strategic vision and “Tone at the Top”

An adviser or fund complex cannot have an effective compliance or ethical culture without a well thought-out strategic vision that incorporates compliance goals and objectives. The development of this culture requires direct input and involvement by a firm’s chief compliance officer (“CCO”) and other members of senior management.

Thus, the first step in coming up with a framework for outlining your firm’s culture of compliance should be for the CCO and senior management to identify the priority areas for compliance to focus its limited resources — initially, and periodically thereafter. This of course does not mean that less significant areas go unattended to; rather, the focus areas should provide compliance personnel with a reasonable set of goals that they can then set out to achieve.

The prioritization of compliance and regulatory risks should be a significant, on-going project for any CCO. However, without buy-in from the highest levels of management, a firm’s strategic vision can be rendered inadequate. One cannot emphasize enough the importance attributed to a firm’s most senior principals setting a personal example such that others will follow their direction and lead. Stephen Cutler, the former Director of the SEC’s Division of Enforcement, didn’t mince words when describing the importance of the “tone at the top” construct[12]:

“You’ve got to talk the talk; and you’ve got to walk the walk. Both are critical to maintaining a good tone at the top . . . You have to talk about the company’s ethical standards again and again. Those standards have to infuse the day-to-day lives of your employees. What does that mean? Ethics and compliance should be part of your regular education and training efforts — and I mean efforts that go beyond perfunctory lectures about legal requirements, but embrace well-conceived, real-life situations and dialogue. It also means that whenever your CEO is delivering a state-of-the-company address to company employees, or offering remarks at a company event, she should be talking about the company’s values as well as its profits . . . What’s more, it has to be senior management — not just the legal department, the compliance professionals, or human resource experts — that does the talking. Matters of ethics and culture shouldn’t be shuttled off to the outer edges (or cost centers) of a corporate organization. In order to convey the importance of integrity and honesty to a corporation’s employees, those who run the business, those who are responsible for the bottom line, have to be the ones to tell employees that integrity and honesty matter. For if they don’t do it, employees won’t believe that those values are core values; they won’t believe that integrity and honesty are important to those who really matter; they won’t believe that their path to success will require adherence to those values . . . And no double talk. You can’t say to the broad audience that ethics, integrity, and honesty are important, but ignore them (or worse yet, joke about them or dismiss them) when you’re in a social setting, or “off line”, or off the record, or when you’re talking to smaller groups . . . What no double talk also means is that if something goes wrong, if there is an ethical or legal lapse, be candid about it, acknowledge it, and don’t try to minimize it. Instead, tell your employees (and the world at large) that it shouldn’t have happened and that it’s inconsistent with the kind of company you want to be.

One of the many “tests” that the SEC staff has indicated they conduct to assess a firm’s culture of compliance is how often, if at all, they identify instances of compliance personnel elevating compliance issues and problems, via memoranda and e-mails, to senior management. Thus, it is incumbent upon an adviser’s senior management and board of directors (when applicable) to accept the responsibility for creating a firm-wide culture of voicing compliance concerns to insure that they get reported and resolved in a timely manner. To accomplish this, firms have begun to create culture-of-compliance committees or have appointed ethics or compliance ombudsmen to serve as an outlet for personnel who want to report issues anonymously. Employees cannot be made to feel as though the reporting of compliance issues will result in retaliation, retribution, or termination. Rather, a firm’s policies and procedures should address the protection of whistleblowers and the ramifications for punishing or harassing such individuals.

In addition, it is important to note that CCOs should have real-time access to senior management, should be involved in the allocation and prioritization of compliance resources, and should proactively develop focused compliance target areas. Questions frequently asked by the SEC’s examination staff include: Where does the compliance department fall on your firm’s organizational chart? Does the chief compliance officer have a
direct reporting line to the CEO or board of directors? Alternatively, does the CCO report to
the head of one of the firm’s business units or someone other than a very senior person within
the organization? The answers to these questions can be very telling of the type of ethical
organization a firm has created. In summary, the interest that senior management shows in
compliant and ethical practices must be real and transparent. Without that “tone at the top,”
a firm’s employees will at best question, or at worst take advantage of, a firm’s supposed
ethics and compliance code.

Risk identification

The second element integral to the development of a culture of compliance is risk
identification. In order to be in a position to establish appropriate internal controls and risk
management and compliance processes, a firm must initially, and at least annually
thereafter, evaluate the risks inherent in its advisory business. As noted in the SEC’s
compliance rule, “Each adviser, in designing its policies and procedures, should first
identify conflicts and other compliance factors creating risk exposure for the firm and its
clients in light of the firm’s particular operations, and then design policies and procedures
that address those risks”[13].

The general purpose of the risk assessment process is to identify key compliance risks and
promptly devise action steps to address those areas. An adviser’s risk assessment process
should attempt to ascertain the inherent level of risk (e.g. low, medium, or high) to the firm
and its clients with respect to general risk areas identified by the CCO. In order to prioritize
all identified risks, the CCO should conduct a general assessment of firstly, the probability of
the risk’s occurrence and secondly, the impact of this occurrence on the interests of the firm
and its clients. Based on these factors, an adviser should attempt to allocate the firm’s
resources to the highest risk areas in an effort to mitigate or control the risks. Finally, a CCO
should periodically analyze information sources to identify compliance risks on a more
frequent basis (e.g. exception tracking entries, proactive review reports, assess regulatory
developments, etc.).

Establishment of controls

In accordance with the Investment Advisers Act of 1940, registered advisers must adopt
comprehensive compliance programs that are reasonably designed to detect, prevent, and
correct violations of the Advisers Act, and any other federal and state securities laws
relevant to the firm’s advisory business[14]. The SEC indicated that the policies, procedures,
and controls that are established by a firm should address the following key compliance risk
areas to the extent they are relevant to the adviser:

- portfolio management processes, including allocation of investment opportunities
  among clients and consistency of portfolios with clients’ investment objectives,
  disclosures by the adviser, and applicable regulatory restrictions;
- trading practices, including procedures by which the adviser satisfies its best
  execution obligation, uses client brokerage to obtain research and other services
  (“soft dollar arrangements”), and allocates aggregated trades among clients;
- proprietary trading of the adviser and personal trading activities of supervised
  persons;
- the accuracy of disclosures made to investors, clients, and regulators, including
  account statements and advertisements;
- safeguarding of client assets from conversion or inappropriate use by advisory
  personnel;
- the accurate creation of required records and their maintenance in a manner that
  secures them from unauthorized alteration or use and protects them from untimely
  destruction;
- marketing advisory services, including the use of solicitors;
- processes to value client holdings and assess fees based on those valuations;
safeguards for the privacy protection of client records and information; and
business continuity plans.

A firm's compliance policies and procedures and risk management processes and controls should be customized to address the specific nature of a firm's advisory services and clients, formalized, and documented in writing. It is necessary for compliance personnel to continuously evaluate whether or not the firm is adhering to its own written policies and procedures; there is nothing more frustrating to a regulator – or embarrassing to a compliance professional – than to find a firm that is not following its own internal guidelines and processes.

An adviser will be found to have a deficient culture of compliance if it has adopted grandiose policies and procedures that are inadequate or boilerplate. One former SEC staffer described his view of a non-customized compliance program[15]:

One word of caution, however: many advisers may be tempted to adopt so called “off the shelf” compliance manuals or codes of ethics as their own. This can be a dangerous practice. First of all, a “one size fits all” approach often does not work when it comes to compliance matters. Compliance policies and procedures are most effective when they are tailored to the specific size, structure and operations of your advisory firm. Second, many advisers that borrow generic compliance policies and procedures unwittingly sign on to a particular policy or procedure that they are not prepared to implement – and sometimes not even aware that they have obliged themselves to implement. Be careful to tailor your policies and procedures and your codes of ethics to the individualized circumstances of your own firms.

Accordingly, the SEC's examination staff begins its inspections with the expectation that a firm has established customized controls that are strong enough to catch compliance problems. A compliance officer that tells an SEC examiner that his advisory firm has had no compliance issues over the past certain number of years is likely to make the examiners speculate that, either the compliance officer is not being as truthful as a subsequent review of the documentation will indicate, or the controls established by the firm have been inadequately designed to catch and fix compliance issues. A compliance officer who puts him or herself in this position can expect the SEC's examination staff to stay longer and dig deeper, unless evidence or documentation is provided to support the fact that the compliance program is self-policing and self-remediating.

Documentation

The collection of useful and pertinent information is essential to the continued detection, prevention, and correction of regulatory risks and compliance issues. Once identified and captured, the information gathered by an adviser must then be effectively communicated to the right personnel across the organization for detailed review and analysis.

An adviser's compliance systems should be set up and organized in ways to produce reports and data that contain operational, financial and compliance-related information addressing both internal and external factors that impact the firm's regulatory and compliance risks. The following information is an example of the type of data and reports that can be periodically compiled and reviewed by a compliance officer to support the continuous assessment of a firm's risk environment:

- Financial statements (review of audited financials, if applicable, and general ledgers for the adviser, private investment funds, etc.).
- Periodic compliance reports (surveillance reports, supervisory reviews and email reviews).
- Exception reports.
- Reconciliation reports.
- Compliance certifications.
- Reports provided by third-party experts (consultants, auditors, or attorneys).
- Service provider reports.
- Regulatory inspection letters (e.g. SEC).
The identification of risks and actual or potential compliance concerns should be the responsibility of every employee. The employees who comprise an adviser’s business units are on the front lines and are in the best position to identify real-time issues or concerns. Accordingly, all employees should be instructed to exercise good judgment and to bring compliance-related concerns promptly to the attention of the CCO or a member of a firm’s senior management and to be alert for any actual or potential conflicts of interests with clients.

**Accountability**

The final element of a culture of compliance is accountability. It is no longer good enough, as it was years ago, for a firm’s policies and procedures to indicate that the “firm” will do this or the “firm” will do that. The SEC now wants a firm’s compliance program to be detailed with the names or titles of those who are responsible for the successful implementation and oversight of key compliance and regulatory risk areas. The buck ultimately has to stop somewhere; now the SEC wants to know with whom it stops[16].

Any material issues that are ultimately brought to the attention of a chief compliance officer or senior management are typically escalated up to the CEO of the firm and/or the firm’s outside advisers or outside counsel. The new requirements of Rule 206(4)-7 under the Advisers Act has fostered the promotion of regular and meaningful interaction between an adviser’s CEO and the CCO – including periodic meetings, reporting, and consultations regarding the company’s compliance processes and systems.

**Self-reporting and cooperation**

One final issue worth noting is the concept of an advisory firm enhancing its culture of compliance by self-reporting regulatory and compliance violations, issues, and problems to the SEC and cooperating with regulatory agencies during formal investigations. There have been several recent examples of cases where it appears as though self-reporting and cooperation with the SEC staff have been instrumental in the avoidance of enforcement actions. For example, the SEC acknowledged that it did not bring an enforcement action against Putnam Fiduciary Trust Company (“PFTC”) because of “swift, extensive and extraordinary cooperation” including[17]:

- prompt self-reporting;
- an independent internal investigation;
- sharing the results of that investigation with the government (including not asserting any applicable privileges and protections with respect to written materials furnished to the Commission staff);
- terminating and otherwise disciplining responsible wrongdoers;
- providing full restitution to its defrauded clients;
- paying for the attorneys’ and consultants’ fees of its defrauded clients; and
- implementing new controls designed to prevent the recurrence of fraudulent conduct.

In addition, we have not seen an enforcement action taken against Circle T Partners, a well-known hedge fund manager that reported to the SEC a matter involving unauthorized trading by one of its employees that resulted in $12 million of losses[18]. Among other things, Circle T Partners took the following actions that would appear to garner high culture of compliance marks from regulators:

- provided immediate notification to the SEC upon discovery of the issue;
- fired the employee involved in the violative conduct;
- conducted an internal review at the firm’s own cost;
- disclosed the matter to investors;
- continued to cooperate with the SEC; and
- provided full restitution to investors for their losses.
An SEC Staff member expounds upon the above examples with the following remarks that were given less than one year ago[19]:

Finally, I would like to say a few words about self-reporting compliance problems and cooperating with the SEC in investigating and resolving problems. As I mentioned, SEC examiners specifically request that firms self-report on any material compliance breaches during comprehensive compliance examinations. In October 2001, the SEC issued a Report of Investigation and Statement explaining its decision not to take enforcement action against a company it had investigated for financial statement irregularities. In so doing, the Commission articulated a framework for evaluating cooperation in determining whether and how to charge violations of the federal securities laws. The Report identifies four broad measures of a company’s cooperation:

- self-policing prior to the discovery of the misconduct, including establishing effective compliance procedures and an appropriate tone at the top;
- self-reporting of misconduct when it is discovered, including conducting a thorough review of the nature, extent, origins and consequences of the misconduct, and promptly, completely, and effectively disclosing the misconduct to the public, to regulators, and to self-regulators;
- remediation, including dismissing or appropriately disciplining wrongdoers, modifying and improving internal controls and procedures to prevent recurrence of the misconduct, and appropriately compensating those adversely affected; and
- cooperation with law enforcement authorities, including providing the Commission staff with all information relevant to the underlying violations and the company’s remedial efforts.

The criteria are set forth in greater detail in the 21(a) Report issued in connection with the above case. Reduced charges, lighter sanctions, or mitigating language in documents the Commission uses to announce and resolve enforcement actions are examples of possible results of cooperative behavior and self-reporting. Enhanced communications between financial firms and regulators is another positive step in rebuilding ethics and compliance in the securities industry through appropriate prompt responses to compliance issues and early resolution of problems. We look forward to continuing progress in opening the lines of communication between our staff and securities firms[20].

Firms should consider self-reporting and cooperation with regulators only after having first discussed the matter with competent and knowledgeable legal counsel. To proceed in any other manner and without first taking steps to remedy a problematic compliance situation could lead to more significant issues with the SEC or another regulatory agency.

Conclusion

The concept of a “culture of compliance” is subjective and intangible. It is difficult to think about, hard to document, and even more complicated to explain to an SEC examiner. A firm cannot just go out and get a culture of compliance during an SEC inspection – you cannot “just do it.” A culture of compliance has to be something that is ingrained in the daily rituals of each of the firm’s employees, including senior management, who must learn to lead by example. A real culture of compliance consists of the day-to-day decisions and actions that take place when no one is looking.

Notes

3. See, Tone at the Top: Getting it Right, Stephen M. Cutler, Director, Division of Enforcement, US Securities and Exchange Commission, December 3, 2004, at: www.sec.gov/news/speech/spch120304smc.htm. As noted in this speech, from October 1, 2002 through September 30, 2004, “... the SEC has brought more than 1,300 civil cases and has obtained orders for disgorgement and penalties in excess of $5 billion. These numbers far exceed those of any other
two-year time frame in the Commission’s history. In this same period, the Department of Justice has brought criminal cases alleging securities-related misconduct by more than 500 defendants.”


5. See the Institutional Shareholder Services’s “Corporate Governance Quotient” and GovernanceMetrics International’s Rating Reports.


16. In the end, a firm’s senior management is accountable for all of the activities that occur under their watchful eye. As noted in an SEC speech, “The responsibility for risk management and compliance with securities laws in the US rests first with the firms themselves and their senior management. The risk management buck stops at the top.” See, Compliance and Internal Controls – Key Priorities for US SEC Examination Program, Mary Ann Gadziala, Associate Director, Office of Compliance Inspections and Examinations, US Securities and Exchange Commission, September 23, 2002 at: www.sec.gov/news/speech/spch583.htm


To purchase reprints of this article please e-mail: reprints@emeraldinsight.com
Or visit our web site for further details: www.emeraldinsight.com/reprints