Information Systems Security, 16:357–361, 2007
Copyright © Taylor & Francis Group, LLC
ISSN: 1065-898X print/1934-869X online
DOI: 10.1080/10658980701805050

Taylor & Francis
Taylor & Francis Group

Regulatory Compliance and the Chief Compliance Officer

Edward H. Freeman, JD, MCP, MCT
West Hartford, CT, USA

> Character is doing the right thing when nobody is looking. There are too many people who think that … the only thing that's wrong is to get caught.
>
> J.C. Watts

The public disgrace and downfall of once-respected corporations such as Enron, Arthur Andersen, and WorldCom cost the economy and innocent parties billions of dollars. Legislation requiring tight restrictions on corporate behavior soon followed. To conform to these tight new regulations, the role of chief compliance officer (CCO) has taken on new importance in the corporate environment. The CCO has long existed at organizations "that operate in heavily regulated industries such as financial services, government agencies and health care".[1] Legislation such as the Sarbanes-Oxley Act (SOX) and the recommendations of the U. S. Federal Sentencing Guidelines have made accounting responsibility more crucial and made the CCO a necessity in any firm.

"Every major corporation in America has, as a stated goal, the need for an effective corporate compliance program."[2] The lack of an effective compliance program may result in criminal and civil exposure for a corporation, as well its directors and executives. Establishment and enforcement are essential for the ongoing success of any major organization today. Selecting a CCO to manage and maintain this program effectively is an integral part of this process.

"It is critical that firms establish a strong culture of compliance that guides and reinforces employees as they make decisions and choices each day."[3] Federal guidelines demand that firm corporate compliance regulations be in place and enforced. The Federal Sentencing Guidelines state:

> Convicted individual agents of organizations are sentenced in accordance with the guidelines and policy statements in the preceding chapters. This chapter is designed so that the sanctions imposed upon organizations and their agents, taken together, will provide just punishment, adequate deterrence and incentives for organizations to maintain internal mechanisms for preventing, detecting and reporting criminal conduct.[4]

This article deals with the role of the CCO in the corporate environment and how this position is crucial in creating and maintaining the security of sensitive corporate information. It also discusses the requirements for hiring

Address correspondence to
Edward H. Freeman,
92 Lawler Road,
West Hartford, CT 06117.
E-mail: edfreeman@hotmail.com

a CCO and the support necessary from senior management in making this role successful.

RESPONSIBILITY FOR CORPORATE COMPLIANCE

A corporate compliance program is a system designed to detect and prevent violations of law by the agents, employees, officers, and directors of a business. An effective compliance program is not limited to corporations. All business entities, including partnerships and nonprofits, should establish such a plan.[5]

In 1991, the federal government enacted the Organizational Sentencing Guidelines (Chapter 8 of the Federal Sentencing Guidelines). Chapter 8 is an effort to make the penalties for corporate crime both uniform and predictable, to encourage "good corporate citizenship." Penalties under the guidelines include fines, imprisonment, and corporate probation. These penalties are mandatory when a business does not have an effective compliance program. Corporate probation involves intense federal monitoring of the organization and mandatory adoption of a compliance program designed by the government. Such a plan is often far more expensive and probing than a voluntary compliance program would have been.

The guidelines take a "carrot and stick" approach in order to encourage businesses to police themselves. They assign a base fine for each violation, which can be increased or decreased based upon certain aggravating or mitigating factors. The existence of an effective corporate compliance program is one such mitigating factor. An organization with such a program may receive a substantially reduced fine and may be able to avoid corporate probation and criminal prosecution altogether. The guidelines contain detailed criteria that must be satisfied if a compliance program is to be effective.

Courts have established personal liability for corporate directors when their corporations have failed to comply with applicable legal standards. In a 1996 decision by the Delaware Court of Chancery,[6] the court clearly defined and established a director's duty of care to prevent employee oversights. "A director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that failure to do so under some circumstances may, in theory at least, render a director liable for losses." Because it created the possibility of personal liability for misconduct by directors (and heavy fines and imprisonment for the directors themselves), *Caremark* forced directors to be sure that their organizations comply with applicable laws.

Under the Federal Sentencing Guidelines, organizations that create an effective compliance program to prevent and detect violations of the law can minimize prescribed fines. Organizations that condone or tolerate previously criminal activity will receive more severe punishments.[7] As originally adopted, the guidelines define an "effective program to prevent and detect violations of law" as a "program that has been reasonably designed, implemented, and enforced so as to prevent and detect the instant offense." The 1991 guidelines provide that the "hallmark" of an effective program is "that the organization exercise *due diligence* in seeking to prevent and detect criminal conduct by its employees and other agents"[8] (emphasis added). Due diligence requires "at a minimum" that the organization adopt a compliance program. The courts will consider a company's compliance program effective only if it meets the following minimum standards:

1. The company must establish a compliance and ethics program.
2. The board of directors (or other applicable governing body) must be knowledgeable about the program and must exercise reasonable oversight; high-level company personnel must ensure that the program is effective; and personnel entrusted with the day-to-day implementation of the program, who are to be accorded the resources necessary to discharge their duties, must periodically report to high-level employees and to the board of directors on the program's effectiveness.
3. The company must not employ persons in positions of substantial authority (high-level personnel and personnel who exercise substantial discretion or supervisory authority within the company) who have engaged in illegal activity.
4. The company must have a training program through which appropriate compliance and ethics information is disseminated to employees, managers, high-level personnel, board members, and where appropriate, company agents.

5. The company must take reasonable steps to audit, monitor, and evaluate the effectiveness of the program and to provide employees with a means to report violations without fear of retaliation (e.g., an anonymous hotline).
6. The program must be consistently enforced through employee incentives for compliance and disciplinary measures for violations.
7. When criminal activity is discovered, the company must respond appropriately to prevent future violations, including modifying its compliance program as necessary.[9]

ROLE OF THE CORPORATE COMPLIANCE OFFICER

In 1995, Securities and Exchange Commission (SEC) Commissioner Richard Y. Roberts emphasized the need for a single point of authority to oversee the corporate compliance program. Such a program can only be effective if the CCO has the authority to:

> remedy inappropriate conduct. This authority should include the ability to sanction, or maybe even fire, rogue employees. At a minimum, there should be the ability to notify and follow up with supervisors all the way up to the top of the chain of command until the problem is remedied.[10]

The commissioner continued that the CCO must have certain basic "weapons in her arsenal." She must have the authority to remedy in appropriate conduct with ability to sanction. There should be strong, pre-established procedures for monitoring activities of employees and a commitment to enforce them. Management must provide the necessary resources to be effective, even if it is unlikely to have an immediate tangible benefit to an organization. Finally, the overall scheme should emphasize vigilance in monitoring for questionable conduct and taking early action to minimize the harm done.

SARBANES-OXLEY AND THE CHIEF COMPLIANCE OFFICER

After the Enron scandal and the subsequent dissolution of Arthur Anderson, investor skepticism and increased scrutiny led other corporate accounting scandals (WorldCom and Adelphia Communications). The Sarbanes-Oxley Act of 2002 (commonly referred to as SOX), was signed into law on July 30, 2002. SOX quickly became one of the most significant legislative changes to federal securities law since the Great Depression. The Act targets corporate corruption and seeks to restore investor trust in U.S. corporations. It focuses on disclosure, risk management and the auditing and reporting of financial information to investing communities and to the SEC.

SOX's most significant provisions address financial reporting, corporate accountability, and the role of the independent auditor. Its most important provisions of include:

- Accelerated reporting of trades by insiders
- Public reporting of CEO and CFO compensation and profits
- Auditor independence and a prohibition on audit firms offering value-added (read "conflict of interest") services
- Companies are now required to have an internal audit function, which must be certified by external auditors
- Certification of financial reports by CEOs and CFOs

SOX requires that CEOs and CFOs personally certify the accuracy of financial statements. This has increased executive accountability, especially since the submission of false statements may result in as much as 20 years in jail. As an additional precaution, executives and directors may not obtain personal loans from their corporations.

Other provisions require auditor independence and a prohibition on auditing firms offering value-added, business-consulting services. Public companies must also have an internal audit group, certified by external auditors. SOX established the Public Company Accounting Oversight Board to regulate auditing practices.[11]

Corporations of all sizes responded by hiring ethics consultants, creating chief compliance officer positions, establishing committees to handle complaints of misconduct, and issuing corporate codes of ethics. Some corporations hoped that the appearance of an ethical business environment would convince federal prosecutors if uncomfortable situations did develop. These actions were often merely

window-dressing and did little to create an ethical organizational culture or to cause the public to have more faith in "Corporate America."

Often referred to as "corporate cops,"[12] the long-term role of the CCO in major organizations is in transition. "The responsibilities of the position often include leading enterprise compliance efforts; ensuring compliance with internal standards and state and federal laws; managing audits and investigations into regulatory compliance issues; and responding to requests for information from regulatory bodies."[13] There is even a Chief Compliance Officer University (www.ccouniversity.org), where individuals can become Certified Compliance Officers and receive a Masters Certificate in Advisor Compliance.

A recent job advertisement for a CCO required a law degree, five years as a senior compliance officer. Other principal duties included the following:14

- Manage team of two compliance specialists and one licensing specialist. The chief compliance officer will provide information with respect to compliance activities to the chief executive officer and senior management of company and the residential mortgage desk and the legal and compliance department of parent company.
- Work with the general counsel and the internal audit function of company to prepare a compliance program and implement the program. Work with each business unit to develop effective compliance training and execution.
- Works with state regulators to establish and maintain excellent relationships both pre and post exam.
- Management of compliance issues including monitoring changes in applicable state, local and federal laws, regulations, and implementing appropriate changes to company practices (including, without limitation, fees charged and disclosures made to borrower and general compliance practices of company and the ancillary businesses related thereto).
- Company has an approach to risk management that includes the office of the general counsel, the compliance officer, and the servicing risk management function. The chief compliance officer is a critical part of this team and must have excellent communication skills (written and oral), ability to work under short deadlines and crisis management conditions, a strong and professional presence and a solid working knowledge of the applicable laws.

It is obvious that ethical conduct and compliance must be an integral part of a firm's culture. A CCO's daily responsibilities require tact, a sense of humor, executive support and above all, an unquestioned level of ethical conduct. A successful CCO will act as an educator and advisor. She must deal with all levels of management, corporate employees, government regulators and the public with respect, diplomacy, and discretion. Her ultimate goal is to create an environment where employees are likely to act properly, even when the regulators are not looking.

CONCLUSIONS

Enron forever changed the public perception of corporate misconduct. SOX added a new dimension to the requirements of ethical behavior in business. Senior executives are putting not only their own integrity and their organization's reputation on the line. They are also risking their personal freedom when they fraudulently misrepresent their organization's financial condition. A skilled CCO, running a successful compliance program, can serve as a voice of reason and integrity when the perceived demands of business conflict with business ethics and regulatory constraints.

Even the most efficient chief compliance officers cannot eliminate all white-collar crime. Organizations must realize that corporate culture where employees align their conduct with regulatory and ethical standards, as defined by the CCO, will prevent the organization from undergoing the problems caused by questionable conduct in today's marketplace.

BIOGRAPHY

Edward H. Freeman, JD, MCP, MCT (edfreeman@hotmail.com) is an attorney and educational consultant in West Hartford, Connecticut. He has written over 50 articles on computer technology, privacy, security and legal issues. He is also an adjunct faculty member at Central Connecticut State University, St. Joseph College in West Hartford, Connecticut, and the University of Connecticut.

NOTES

1. Dov Seidman, *Do You Need a Chief Compliance Officer?*, InformationWeek, February 18, 2005.
2. Marc S. Raspani and Gregg W. Mackuse, *What's Really So Important about an Effective Compliance Program?",* 31 National Association of Criminal Defense Lawyers, The Champion 12, May 2007.
3. Ashoke S. Talukdar, *The Voice of Reason: The Corporate Compliance Officer and the Regulated Corporate Environment*, 6 University of California, Davis, Business Law Journal 45, Fall 2005.
4. *U.S. Sentencing Guidelines Manual, Chapter 8 – Sentencing of Organizations* (2005).
5. See www.corporatecompliance.com/faq.htm. (Visited October 20, 2007).
6. *In re Caremark International Inc. Derivative Litigation,* 698 A.2d 959 (Del. Ch. 1996).
7. Paul Fiorelli, *Will U.S. Sentencing Commission Amendments Encourage a New Ethical Culture Within Organizations?*, 39 Wake Forest Law Review 565 (Fall 2004).
8. U.S. Sentencing Guidelines Manual 8A1.2 cmt. n.3(k) (1991) (amended 2004).
9. Melvin S. Schwechter and Stephen A. Best, *US Sentencing Commission Raises Minimum Standards for Compliance Programs: Companies Will Find It Tougher to Make the Grade*, Banking & Financial Services Policy Report, July, 2004.
10. http://www.sec.gov/news/speech/speecharchive/1995/spch030.txt. (Visited October 20, 2007).
11. Cristina Michelle DeCelestino, *Krispy Kreme, Sarbanes-Oxley, and Corporate Greed*, 15 University of Miami Business Law Review 225, Spring/Summer, 2007.
12. Joseph Weber,*The New Ethics Enforcers: These corporate cops have unprecedented power to throw their weight around*, Business Week (February 13, 2006).
13. Seidman, supra note 1.
14. http://www.complianceweek.com/index.cfm?fuseaction=article.viewJobPosting&article_ID=2463 (Visited October 20, 2007). See also www.ache.org/newclub/career/comploff.cfm.

Copyright of Information Systems Security is the property of Taylor & Francis Ltd and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.