NSCP CURRENTS
A Publication of the NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS

The Evolving Role of The CCO and What It Means

by Lorna A. Schnase and Robert V. Coulter

The role of the CCO has been evolving ever since the rules were adopted requiring their appointment.[1] This article reflects on how that role has changed and discusses various issues deserving renewed attention as a result.

How Has the Role of the CCO Been Evolving?

Many changes have occurred over the years but among the most significant has been a shift in the CCO's primary role from that of *supervisor*, responsible for overseeing others in the firm from a compliance standpoint, to that of *compliance program director*, responsible for designing, implementing and testing the firm's policies and procedures, as contemplated by applicable rules.[2] Increasingly these days, supervision is recognized as more appropriately undertaken by experienced personnel at the business unit level, rather than by personnel from the compliance area.

A similar shift has occurred in the CCO's principal function from that of *document producer*, responsible for creating the documents that comprise the firm's compliance program,[3] to that of *risk manager*.[4] Now more than ever, CCOs are considered a key player – if not *the* key player – in the effort to identify, assess and mitigate risk in their firms.

What Does This Change Mean for CCOs?

A number of things, among them:

• CCOs are increasingly expected to be educated, trained and treated like professionals in their own right. In past years, more than a few CCOs have been hastily appointed to their positions simply to satisfy rule requirements calling for a CCO. Undoubtedly, many found themselves ill-prepared, if not unqualified, to serve in that role. Increasingly, however, CCOs are accomplished compliance professionals with the background and experience to match. Many are earning certifications or designations as compliance professionals[5] even if they are not full-time CCOs. Numerous professional organizations, conferences, journals and products now exist, specifically aimed at serving financial services professionals in the compliance arena.

• Regulators have followed this evolution and their expectations have evolved along the same lines. In examinations, regulators expect CCOs to be knowledgeable about the firm's business and compliance procedures and to have a solid understanding of how risks are managed in the firm. If there ever *was* a grace period for newly appointed CCOs to get their act together, there is ample evidence that it is long over. Indeed, a number of regulatory actions have now been brought against firms for failure to have an adequate compliance program in place, including actions naming the CCO or other responsible individuals personally.[6]

• There is a newfound sensitivity to risk management and a whole new alphabet soup of acronyms to accompany it. While firms have been urged to think about risk assessment for quite some time,[7] it has taken until recently for them to start talking about risk management in the more comprehensive and integrated way it is now. Today, CCOs are increasingly being asked to familiarize themselves with concepts once considered the

(Continued on page 2)

Lorna A. Schnase *is an independent investment management attorney focusing her practice on matters under the Investment Advisers Act of 1940 and the Investment Company Act of 1940 primarily for registered advisers and funds.* ***Robert V. Coulter****, Senior Vice President and Director of Compliance at First Southwest, contributed to this article adding his insights on broker-dealer compliance and as an incumbent adviser and broker-dealer CCO.*

© 2010 National Society of Compliance Professionals, Inc.

EVOLVING ROLE OF THE CCO
(Continued from page 1)

exclusive province of financial professionals and MBAs, including risk metrics such as VaR (Value at Risk), beta, Monte Carlo analysis and stress testing techniques,[8] and the risks posed by complex products such as MBSs (mortgage-backed securities), CMOs (collateralized mortgage obligations), ABSs (asset-backed securities) and CDSs (credit default swaps) to name a few. At the same time, broad new concepts of risk management have come under discussion, such as ERM (enterprise risk management)[9] and GRC (governance, risk and compliance).[10] On the global stage, the ISO (International Organization for Standardization) has codified a family of risk management standards under ISO 31000:2009, along with guidance on systematic techniques for risk assessment.[11] IOSCO (International Organization of Securities Commissions) has published numerous papers addressing risk management, including a report entitled "Risk Management and Control Guidelines for Securities Firms and Their Supervisors."[12] Overlay onto this the desire of lawmakers and others to address risk systemically in the financial sector as a whole, and risk management seems poised to be a keystone concept for the foreseeable future.

• CCOs are being forced to think about ever more expansive areas, in some cases way outside their comfort zone. In the past, CCOs focused principally on the firm's regulatory obligations under the federal securities laws and geared the compliance program toward ensuring those obligations were met.[13] Today, however, legal and regulatory risks can emanate from many quarters beyond the federal securities laws, including the banking laws, tax laws, FTC rules (such as the "Red Flags Rule"), ERISA (federal retirement plan law), Blue Sky (state securities) laws, state privacy regulations, state and local pay-to-play restrictions, laws protecting seniors and investors with diminished capacity, and so on.[14] As a result, CCOs must be increasingly nimble in getting up to speed on and resolving issues in a wide range of areas.

• Indeed, risk management in the broadest sense can demand expertise way beyond rules and regulations, in fact beyond the skill set of any one ordinary person, into areas such as insurance, portfolio hedging, accounting/audit, IT, business continuity planning and so on. This may have different consequences in different firms. CCOs in smaller firms may find themselves stretched beyond capacity if they try to cover all these different areas and may need to tap outside resources for additional expertise. CCOs in other firms – particularly larger, more complex firms – may find themselves repositioned in the firm hierarchy and dealing with a newly appointed Chief Risk Officer hired to coordinate all the professionals addressing these various facets of risk and ensuring seamless risk management enterprise-wide.

How is the CCO's Role Likely to Evolve in the Future?

Most certainly, the line will continue to sharpen between those risks considered the CCO's responsibility (such as regulatory compliance under the securities laws) and those more appropriately considered the responsibility of others with expertise in different areas (such as IT and data security, portfolio hedging, disaster recovery, and so on). Closely related – in firms that have not already addressed the issue – will be deciding who should be responsible for coordinating the various risk areas to avoid gaps.

As risk management adopts more systemic and enterprise-wide concepts, CCOs may see other changes in their role. For example, CCOs may be asked to find opportunities to consolidate operations from a risk perspective, based on an understanding of how regulation in one area impacts other areas. In any case, appropriate use of technology is likely to continue to grow.

Should CCOs be Concerned About Their Exposure to Personal Liability?

Employees would always be wise to understand their personal exposure and what is being done to mitigate it. Indeed, this is one area that warrants renewed attention due to the shift in the CCO's role discussed above. Greater responsibility for key functions, such as risk management,[15] can be expected to carry greater exposure to liability should things go wrong.

Many employees operate under the false impression that they cannot be sued personally for mistakes they make in the scope of their employment, thinking that their employer – and not they – would be held liable. That is not true. No doubt, employers can be held vicariously liable for wrongdoing committed by their employees, but that does not get the employee off the hook. That just makes the employer liable *in addition to* the employee.

So why don't we hear a lot more about employees being sued?[16] For a couple of reasons: First, even if an employee is potentially liable along with the employer, suing parties may choose to aim their claims at the

employer because the employer is likely to have more assets – and perhaps insurance – to satisfy the liability. Second, the employer may have an obligation to indemnify the employee anyway, depending on the circumstances, under the employer's organizational documents[17] or applicable law.[18] So even if employees are sued, they may be joined along with the employer, and the employee's legal representation, amounts paid in settlement, judgment amounts and other costs may wind up being paid by the employer in the end.

While these factors can be helpful if an employee is sued by a private party (like a client), they of course depend on the employer *having* indemnification obligations,[19] *and* sufficient assets or insurance to cover the employer's own liability as well as the employee's. Moreover, it can be difficult for employees to enforce those obligations against their employer if the employee has left the firm under strained or hostile circumstances or if the firm has been seized by regulators.

In addition, indemnification may not be as helpful or even available if the employee is pursued by the SEC, as opposed to a private party.[20] Even SEC civil actions can lead to fines and monetary penalties, as well as suspensions or bars from working in the industry, making it difficult for affected employees to earn a living. While the SEC Staff and FINRA have said they are not gunning for CCOs or attempting to hold them liable for every violation that occurs in the firm,[21] they are clearly willing to name CCOs personally when they believe the case warrants.[22]

What Questions Can CCOs Ask to Better Understand Their Personal Exposure and Available Protections?

Practical questions include:

• Does the CCO's employer provide indemnification protection for employees, in the organizational documents or otherwise?[23]

• If so, what do those provisions say? What kinds of claims, losses and so forth are indemnified? What are the exclusions?

• Will the employer advance the cost of attorney's fees if an employee is sued, prior to a final determination of whether the employee is liable or entitled to indemnification? Legal defense costs can be the biggest single cost an employee faces in a lawsuit.

• Is the employer adequately capitalized to cover any reasonably foreseeable losses? Or, is it chronically running in the red or on razor thin margins without an adequate safety net?

• Does the employer have adequate E&O (errors and omissions) or similar insurance in force to provide reasonable coverage for its operations, including the potential personal liability of any employees acting within the scope of their employment? Likely, the availability and affordability of insurance will vary depending on the firm's size and its sphere of operations. Without insurance, however, everyone is depending on firm assets for coverage.

What Else Should CCOs Consider in Light of their Evolving Role?

CCOs should stay alert to a number of other issues, such as:

• CCOs should make sure that an evolution in their role does not inadvertently result in saddling them with new responsibility for the compliance of other employees. Importantly, each employee should remain responsible for their own compliance. CCOs should take on supervisory responsibility for other employees only in well thought-out circumstances when the CCO is in a position and has the means to oversee their performance. Individuals who take on supervisory responsibilities risk becoming a target for regulatory action if violations occur in their areas.

• CCOs should redouble their efforts to make sure they are getting the education, training and support they need to function in their role effectively. The rapid pace of regulatory change in recent years is not likely to ease up soon. This will require ongoing continuing education and effective support.

• The recent economic crisis has put compensation issues back in the spotlight, as Congress, the SEC and others focus on the incentives built into compensation structures used in the financial services industry. This puts two "blips" on the radar screen for CCOs: First, as part of a risk assessment, CCOs should consider how their firms are compensated and address the conflicts of interest and incentives created by those arrangements.[24] Second, CCOs should consider their *own* compensation arrangements to make sure they are properly incentivized to do their jobs. The more CCOs are concerned that their salary, bonus, performance review or stature in the firm will be diminished if compliance problems are found, the less incentive they have to perform robust compliance testing and monitoring. Of course CCOs should be held accountable for their own failings just like everyone else. But firms should make sure that CCOs are properly motivated to ferret out compliance issues diligently and resolve problems

(Continued on page 4)

EVOLVING ROLE OF THE CCO
(Continued from page 3)

efficiently, rather than fear negative personal consequences for all compliance problems uncovered regardless of culpability.

• The economic crisis has raised other challenges for CCOs as well. For example, advisers and dual-registered IA/BDs must remain cognizant of the firm's obligation under the Investment Advisers Act of 1940 to disclose to clients any financial condition that is reasonably likely to impair the ability of the firm to meet its contractual commitments.[25] Broker-dealers, of course, must remain in compliance with their net capital requirements. In these fast-moving and financially stressful times, CCOs should give specific consideration to managing these risks, perhaps monitoring the firm's financial condition more closely to ensure that these obligations are met.

The role of the CCO has evolved over the years from "supervisor" to "compliance program director" and from "document producer" to "risk manager." This will have significant consequences for many CCOs, challenging them to operate in new areas and potentially exposing them to greater personal liability. The information in this article will help CCOs to better understand the nature and implications of these changes and important issues that warrant renewed attention as a result.

1. The SEC adopted Rule 206(4)-7 under the Investment Advisers Act of 1940 and Rule 38a-1 under the Investment Company Act of 1940 requiring advisers and funds to designate a CCO by October 5, 2004. The NASD adopted Rule 3013, now codified in FINRA Rule 3130, requiring broker-dealers to designate a CCO by December 1, 2004.
2. Advisers Act Rule 206(4)-7(c) requires advisers to appoint a CCO responsible for "administering the policies and procedures" adopted by the adviser as directed by the rule. FINRA Rule 3130, Supplementary Material .05 says, in pertinent part: "A chief compliance officer is a primary advisor to the member [firm] on its overall compliance scheme and the particularized rules, policies and procedures that the member adopts."
3. Such as compliance manuals, written procedures, reporting forms, training materials, annual review reports, testing documentation and so on.
4. This is not to imply that documentation is no longer important because it certainly is. But the principal focus of the CCO's role is increasingly on risk management rather than merely on documentation production.
5. For example, NSCP offers a program through which compliance professionals can be awarded the Certified Securities Compliance Professional® (CSCP®) credential. National Regulatory Services and the Investment Adviser Association co-sponsor a program offering compliance professionals the Investment Adviser Certified Compliance Professional (IACCP℠) designation. FINRA offers the Certified Regulatory and Compliance Professional (CRCP) program through the Wharton School at the University of Pennsylvania.
6. See, for example, Battery Wealth Management, Inc. and Wayne Cassady, Release No. IA-2800A (Oct. 15, 2008) (settled); Consulting Services Group, LLC and Joe D. Meals, Release No. IA-2669 (Oct. 4, 2007) (settled); and CapitalWorks Investment Partners, LLC and Mark J. Correnti, Release No. IA- 2520 (June 6, 2006) (settled) (in each case where adviser was found to have violated the adviser compliance rule (Rule 206(4)-7), among other provisions, and the CCO was found to have "aided and abetted" and "caused" the firm's violation). See also Pritchard Capital Partners, LLC, Thomas Ward Pritchard, et al., SEC Administrative Proceeding File No. 3-12753 (Sept. 7, 2007) (managing director/ CCO of broker-dealer was found to have failed to reasonably supervise an employee who engaged in illegal late trading, in part because as CCO he failed to develop written procedures for the firm reasonably designed to detect or prevent that conduct); and FINRA alleged rule violations settled under Letter of Acceptance, Waiver and Consent No. 2007007400504, Westpark Capital, Inc., Respondent, et al. (announced May 6, 2010): "By failing to establish an adequate supervisory system and procedures and by failing to take appropriate action that was reasonably designed to detect and prevent the violations, Westpark [broker-dealer firm], Morgan [CCO], and Stem [COO] violated Conduct Rules 3010 and 2110."
7. See Final Rule: Compliance Programs of Investment Companies and Investment Advisers, Release Nos. IA-2204; IC-26299 (Dec. 17, 2003) at Section II.A.1 (the Adopting Release): "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." See also NASD Notice to Members 99-92, SEC, NASD Regulation, and NYSE Issue Joint Statement on Broker/Dealer Risk Management Practices (November 1999): "The task force has concluded that senior management must play a significant role in the adoption and maintenance of a comprehensive system of internal controls and risk management practices. This role should include the recognition of risk management as an essential part of the business process, management's willingness to fund the necessary elements of a risk management system, including personnel and information technology costs, and recognition that risk management is a dynamic function that must be modified and improved as a firm's business changes and improved processes and procedures become available."
8. See, for example, Richard D. Marshall, "Enterprise-Wide Risk Management for Advisers and Brokers,"

NSCP Currents (November/December 2009).

9. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines ERM as "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." COSO Enterprise Risk Management — Integrated Framework, Executive Summary (2004), p. 2.

10. GRC is a concept that combines the interdependent areas of organizational governance, risk management and compliance, recognizing the need for collaboration among them to achieve entity goals.

11. Downloads of the ISO standards are available on the ISO's website at http://www.iso.org/iso/iso_catalogue.htm.

12. "Risk Management and Control Guidelines for Securities Firms and Their Supervisors" (May 27, 1998) is intended to promote domestic and international risk management and control structure awareness for securities firms and regulators. Among other things, it describes elements of a risk management and control system. It can be accessed on the IOSCO website at http://www.iosco.org/library/pubdocs/pdf/IOSCOPD78.pdf.

13. This was logical, given that the applicable rules technically only require a firm's compliance program to focus on federal securities laws and related rules. See Advisers Act Rule 206(4)-7, FINRA Rule 3130 and NASD Rule 3012.

14. See Bibb L. Strench and Sylvia N. Harris, "Non-Securities Regulations Continue to Rain Down on Securities Firms: Regulation S-AM is the Latest," *Practical Compliance & Risk Management for the Securities Industry* (January-February 2010) at p. 15.

15. This is particularly true in new areas where CCOs may be stretching their expertise.

16. Actually, we do hear about employees being sued even if we don't think about it in that way. For example, all the suits brought against Ken Lay, Jeff Skilling and the other Enron executives were suits for actions taken in their capacity as corporate officers and employees. Bernie Madoff and employee Frank di Pascali were both charged personally for their involvement in the scandal embroiling Madoff's securities firm. Similarly, the fraud charges filed by the SEC against Goldman Sachs in April 2010 were filed against Goldman employee Fabrice Tourre as well as against the firm. For SEC actions brought against ordinary individual CCOs, see the actions cited in footnote 6 above.

17. Indemnification provisions may appear in such places as the firm's articles of organization, bylaws, operating agreements, employment agreements or other similar documents.

18. Some states have enacted statutes requiring employers to indemnify employees under certain circumstances. See, for example, California Labor Code Section 2802.

19. Corporate indemnification statutes may require a corporation to indemnify a corporate representative for expenses incurred in defense of a proceeding brought as a result of serving the corporation if the representative is successful in the defense. Indemnification beyond that is usually permissive and not mandatory, leaving it up to each organization whether and how much indemnification to provide. Statutes vary for organizations other than corporations. See generally "Corporate Indemnification Agreements: Selected Issues to Consider," Kirkpatrick & Lockhart (2003).

20. The SEC has long taken the position that indemnification provisions are unenforceable as against public policy if used to indemnify wrongdoers for certain violations of the federal securities laws (such as certain "anti-fraud" provisions). See, for example, Items 510 and 512(h)(3) of Regulation S-K. Also, E&O insurance may not cover acts that are considered "intentional" or "willful" (common allegations in SEC enforcement actions) and generally will not cover any conduct considered criminal. Moreover, regulators may ask individuals to waive or limit their right to indemnification (or insurance) as a condition to settling legal and enforcement actions. See Paul Berger, then Associate Director of the SEC's Enforcement Division, quoted as saying "[a]nyone who settles with us is going to agree not to be indemnified," in footnote 36 of the August 2006 report of the ABA Task Force on Attorney-Client Privilege.

21. Bob Plaze, Associate Director of the SEC's Division of Investment Management at the CCOutreach National Seminar in Washington, DC, November 8, 2005. Also, see the discussion of personal liability generally in Theodore J. Sawicki and Kerry K. Vatzakas, "Chief Compliance Officer Liability: Setting The Record Straight ," NSCP Currents (November/December 2008) at p. 16.

22. See the cases cited in footnote 6 above.

23. Even CCOs who are technically not "employees" but rather are engaged as independent contractors may be entitled to indemnification under the adviser's organizational documents as "officers" or "agents."

24. SEC Chairman Mary Schapiro even sent an open letter, dated August 31, 2009, to broker-dealer CEOs warning them about "enhanced" compensation practices that may create incentives for representatives to engage in violative conduct. Of course, the potential for compensation arrangements to incentivize inappropriate conduct is not unique to broker-dealer firms.

25. Specifically, Rule 206(4)-4 under the Advisers Act makes it fraudulent for any registered investment adviser to fail to disclose to any client or prospective client all material facts with respect to a financial condition of the adviser that is reasonably likely to impair the ability of the adviser to meet contractual commitments to clients, if the adviser has discretionary authority (express or implied) or custody over such client's funds or securities, or requires prepayment of advisory fees of more than $ 500 from such client, 6 months or more in advance. Advisers should also consider whether fiduciary obligations require them to disclose other similar financial conditions even if not technically within the scope of Rule 206(4)-4.

NSCP CURRENTS

is published by the
National Society of Compliance Professionals, Inc.
22 Kent Road, Cornwall Bridge, CT 06754
(860) 672-0843 / info@nscp.org

NSCP Board of Directors

Joan Hinchman, Executive Director, President and CEO

Lee D. Augsburger
Torstein M. Braaten
A. Brad Busscher
Richard T. Chase
Patricia E. "Trish" Flynn
Patricia M. Harrison
Bari Havlik
Ben A. Indek
Michelle L. Jacko
Deborah A. Lamb
David H. Lui
Martha J. Matthews
Selwyn J. Notelovitz
Diane P. Novak
David W. Porteous
David C. Prince
Charles V. "Chuck" Senatore
Kenneth L. Wagner
Craig R. Watanabe
Judy B. Werner
Pamela K. Ziermann

Editor & Layout
Frederick D. Vorck, Jr.

Editor
Joan Hinchman