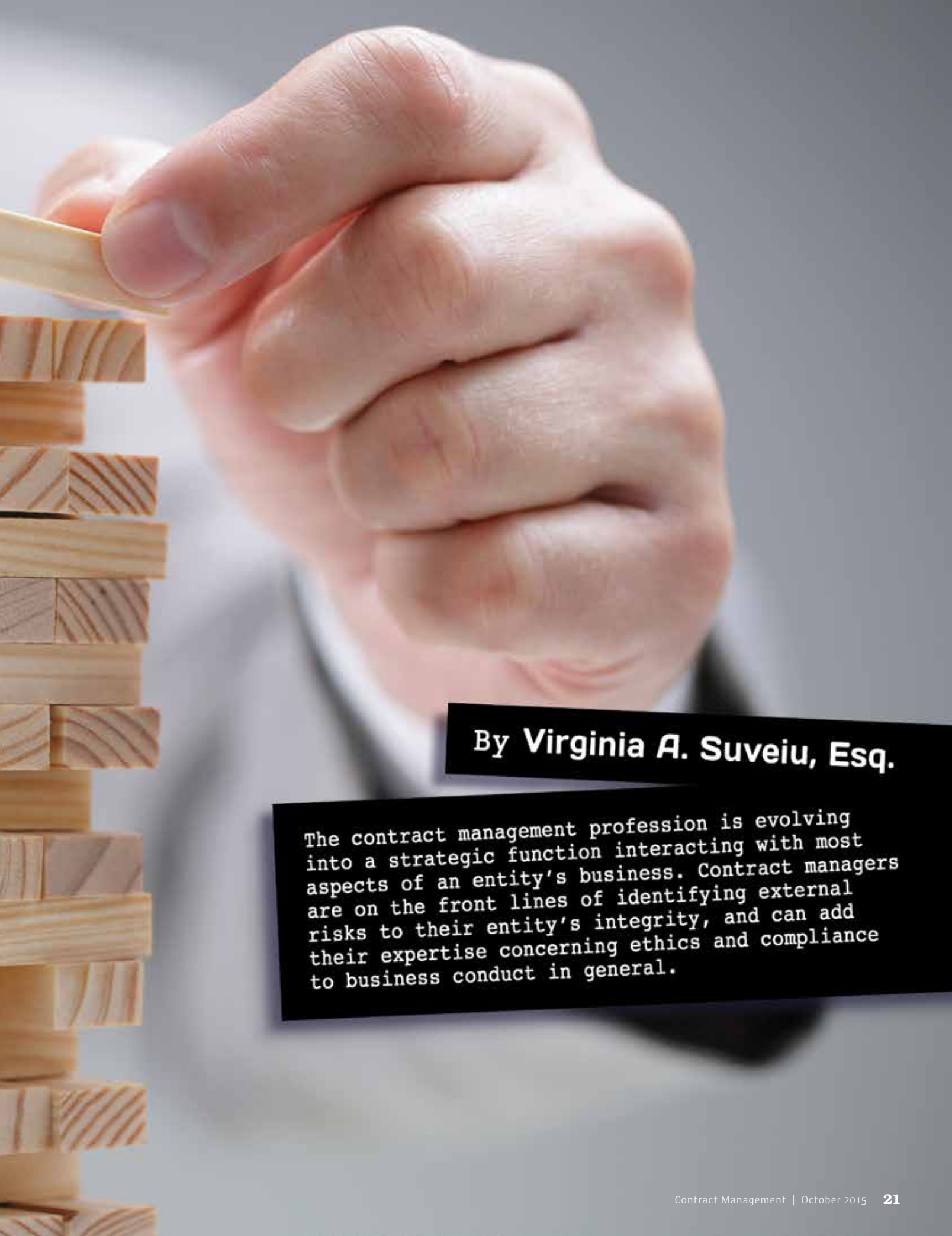
Understanding the Increasing Importance of Contract Risk Management within the Ever-Developing Compliance Function



By **Virginia A. Suveiu, Esq.**

The contract management profession is evolving into a strategic function interacting with most aspects of an entity's business. Contract managers are on the front lines of identifying external risks to their entity's integrity, and can add their expertise concerning ethics and compliance to business conduct in general.

NCMA's *Contract Management Body of Knowledge* (*CMBOK*) states:

> **Other competitors can drive the need to maintain awareness of industry best practices, and, where possible, develop best practices rather than continually implementing those already developed. Again, an efficient and effective contracting process is required to be an industry leader.[1]**

The *CMBOK* goes on to further state: "[o]rganizational influences have a profound effect on the contracting process."[2]

Indeed, the most powerful organizational influence comes directly from the top—i.e., the very top: the board of directors. The *U.S. Federal Sentencing Guidelines* require that boards exercise reasonable oversight in connection with the implementation and effectiveness of the entity's compliance and ethics programs.[3] It is then senior management who "directly influences the initiation of requirements that are ultimately fulfilled through the contracting process."[4]

Yet, compliance and ethics programs rarely receive spontaneous outright support, financial or otherwise, from many a senior corporate leader. Frequently, compliance officers are forced to still build a compelling business case for why the company should invest in a compliance program.[5] The contract manager is, in many entities, still an untapped resource to help build that business case.[6]

The contract manager is well-equipped to assist the organization in achieving contract risk management, which is necessarily the organization's objective.[7] Contract risk management becomes particularly important given that entities increasingly face a vast array of compliance obligations imposed not only by the state, but also by private third parties. For instance, contract clauses and codes of conduct create new compliance obligations and enforcement mechanisms, going into the actual structure of corporate ethics and compliance programs. In many situations, larger companies are now demanding a strong culture of compliance and ethics of small companies, local suppliers, vendors, service suppliers, and banks.[8]

The Compliance Function and GRC

The importance of compliance and the extent of liability for its failure have greatly increased, especially over the last few decades, both in the United States and abroad. Governments possess incredible powers of enforcement and authority to impose heavy penalties, often with only limited judicial involvement.[9]

Working to research, develop, and maintain a robust compliance system is no small task. Legal scholarship on the law of compliance is as of yet underdeveloped.[10] While a heavy burden, this simultaneously creates an opportunity for the contract manager's voice to be heard by senior management, given that the compliance function increasingly involves representations, commitments, rights, and obligations contained in various contractual agreements, all of which the contract manager is already strongly familiar with.

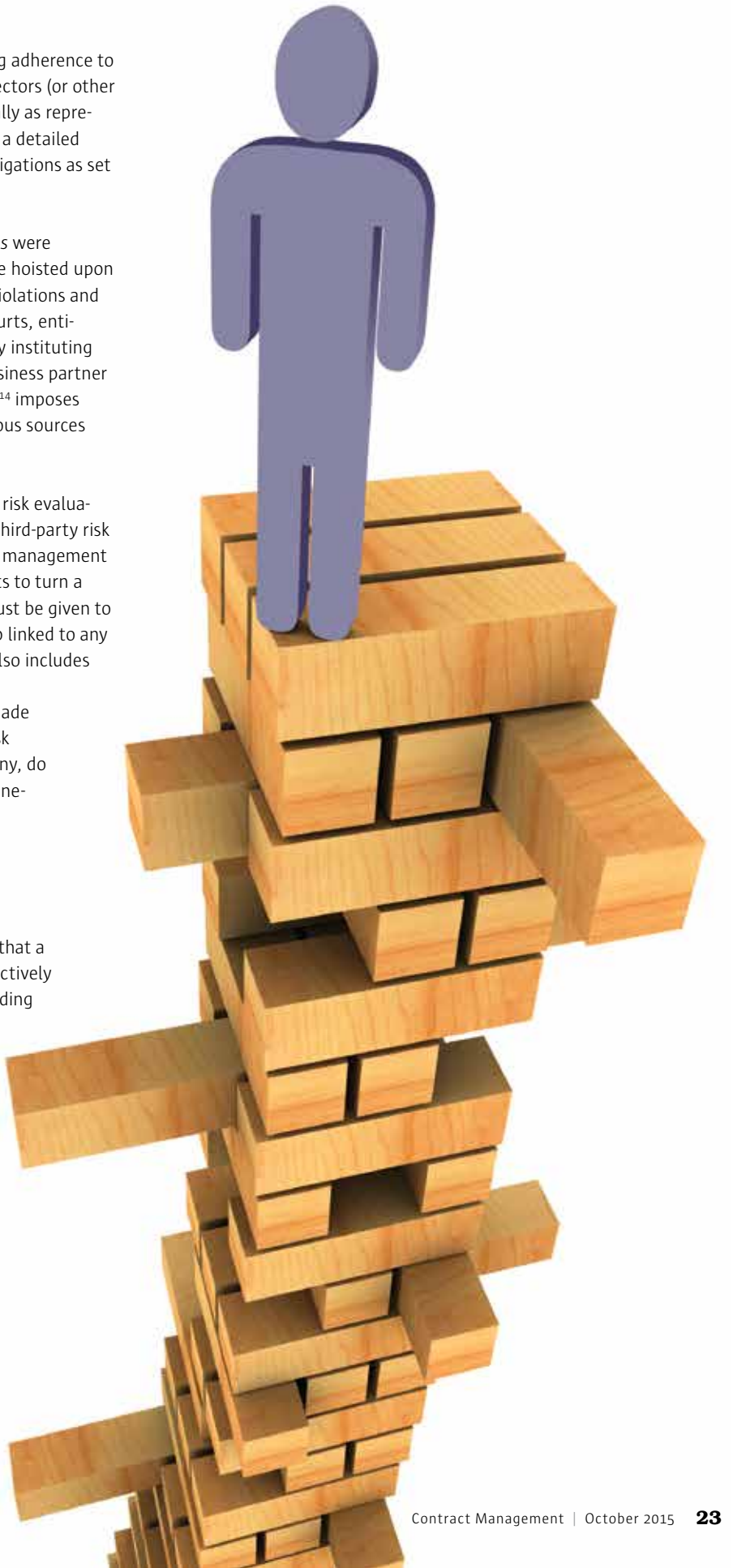
The contract manager can, if he or she does not already, play a vital role in helping to develop, maintain, and improve an entity's governance, risk management, and compliance (GRC).[11] Compliance, together with the closely related fields of governance and risk management, is an essential internal control for corporations and other complex organizations. The compliance function consists of efforts entities take to ensure that employees and business partners do not violate any applicable rules, regulations, or norms.

The compliance function is generally implemented through compliance policies, programs, and, more recently, contracts, especially with third parties. A compliance

policy is a statement of an entity's approach to ensuring adherence to its normative obligations, approved by the board of directors (or other managing body), and announced internally and externally as representing the entity's approach. A compliance program is a detailed statement of how the entity intends to carry out its obligations as set forth in its policy.[12]

Since the *Federal Sentencing Guidelines for Organizations* were established, an element of internalization of compliance hoisted upon private entities has existed.[13] Facing stiff penalties for violations and significantly reduced power to defend themselves in courts, entities have a strong incentive to internalize compliance by instituting effective procedures to guard against employee and business partner misconduct. Moreover, "private-to-private" compliance[14] imposes new forms of risks on entities that may come from various sources such as suppliers, customers, and/or insurers.

Usually, contract risk management consists of contract risk evaluation as well as other data analytic services to enhance third-party risk management and contract compliance. Third-party risk management is a critical component here. If an entity decides it wants to turn a compliance code into a contract, then consideration must be given to the reasonableness, proportionality, and draftsmanship linked to any other current contract obligation. Such consideration also includes the core activities of contract managers like contract formation, negotiation, and other strategic decisions made within cross-functional or integrated process teams. Risk transfer situations, which need to be under strict scrutiny, do exist where procurement and legal staffs have moved one-sided contract terms into their codes.[15]



Understanding What Does and Doesn't Work

Compliance, as a form of internal control, presupposes that a well-managed organization is one where assets are effectively deployed to serve the organization's objectives. The leading statement of internal control is set forth by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).[16] COSO explains:

> [Internal control is] a process, effected by an entity's board of directors, management, and personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.[17]

The pre-Global Financial Crisis of 2007–2008 mentality was to focus squarely on an entity's failure to comply.[18] Many organizations have used a traditional form of what is generally known as "enterprise risk management" (ERM) in the attempt to improve risk management capabilities, including the handling of contract risks. ERM programs

purport to focus on identifying, measuring, and reporting on an organization's top risks. However, ERM is criticized for "completely" missing entity-threatening risks.[19]

However, many an entity still maintains a pre-2008 mentality when it comes to managing risk. The shortcoming of ERM is that it does not meet the goal of increasing the certainty that the organization's objectives, including contract compliance, will be achieved with a tolerable level of risk to the organization's senior management and its board. In the usual lines of defense, an entity will have persons/offices charged with carrying out the monitoring and control activities along with internal audits. Yet, these common lines of defense are supposed to operate as independent checks on the entity, but simultaneously themselves are part of the management team.

Such a set-up fails to take into account other important controls serving to catch and correct problems that slip through the cracks of an internal audit:

- The board of directors (especially the audit committee),
- The external auditor, and
- For regulated firms, the government supervisor.

Moreover, the concept of internal control can include activist shareholders, proxy advisory firms, takeover bidders, and the press—all of whom uniquely monitor the behavior of the organization's managers.

A contract manager is poised to help accurately identify and assess risk, including expected and plausible risks.[20] Given the ever-growing strategic role a contract manager plays, a contract manager can assist in matching the level of risk management sophistication of the entity to the demands of that entity's environment.[21] Thus, the more dynamic and complex the entity's risks actually are, the more sophisticated and mature its risk management processes must be. For mid-sized to larger companies, it is better to consider compliance and ethics as a separate function from the legal function, as this allows for specific focus on risk and culture, not just the law.[22] The aforementioned also allows for sharper focus on the entity's business strategy, with consideration being given to the following factors.

Given the ever-growing strategic role a contract manager plays, a contract manager can assist in matching the level of risk management sophistication of the entity to the demands of that entity's environment.

Compliance Programs *Affected* by Private Litigation

Shareholder derivative suits challenging misconduct sometimes terminate in settlements, whereby the corporation commits to implementing reforms to internal governance. Compliance obligations can also be included in settlements of *qui tam* litigation, such as provisions of the False Claims Act, brought by private parties in the name of the government.[23]

Implementation of Effective Compliance Programs Helps to Mitigate the Severity of Enforcement

Regulators consider an entity's commitment to compliance when they determine whether to commence enforcement actions.[24] Such compliance programs must consider:

- Whether the entity's compliance plan is formal and well-documented;
- Whether it is actively supported by senior management;
- Whether it includes formal training of employees;
- Whether there are audits, both internal and external, of compliance; and
- How the entity responds to violations, such as disciplinary action.[25]

An entity's compliance-related conduct is also taken into account at the penalty stage. For example, the Environmental Protection Agency's program will completely waive a civil penalty for a violation that is detected, reported, and remedied through a systematic compliance monitoring system.[26]

Deferred Prosecution *Agreements* & Non-Prosecution *Agreements*

They may both contain agreed statements of facts, but do not require an admission of guilt. Essential to both of these agreements is the entity's commitment to cooperate with the government and to rectify all deficiencies, including establishing or enhancing compliance programs, policies, and procedures.[27]

Setting the Tone at the Top with Some Help from the Contract Manager

Increased regulations resulting from such business catastrophes like Enron and Lehman Brothers have complicated corporate governance matters, with some directors saying Sarbanes-Oxley now much

more emphasizes the board's responsibility to ask important questions to follow through.[28] Board members should not only be current and knowledgeable about pressing issues facing the corporation, but they should also be fully aware of their duties so as to prevent running afoul of applicable regulations. The board's responsibility for directing the management of a corporation includes a duty to oversee the activities of employees to ensure compliance.[29] In addition to liability for breach of fiduciary duty, directors may face exposure under regulatory statutes for failure to exercise oversight over compliance.[30] Furthermore, the *U.S. Federal Sentencing Guidelines* require that boards exercise reasonable oversight on the implementation and effectiveness of the entity's compliance and ethics program.[31]

Some compliance obligations are imposed on senior managers.[32] Subject to board oversight, the CEO is the face of the company, ultimately responsible for the compliance decisions taken. Thus, it is vital to foster a culture of compliance that includes the practice of listening to what is being said by all employees. Again, contract managers can play an increasingly more active role here.[33] It is important to note that a larger percentage of whistleblowers have stated that they reported suspected violations internally *before* going to the government.[34]

The contract management profession is evolving into a strategic function interacting with most aspects of an entity's business.[35] Contract managers are on the front lines of identifying external risks to their entity's integrity, and can add their expertise concerning ethics and compliance to business conduct in general.[36] **CM**

ABOUT THE AUTHOR

VIRGINIA A. SUVEIU, ESQ., counsels on legal risk management, regulatory compliance, and commercial and international law matters. She is also an instructor at UC Irvine Extension for the Contract Management Certificate Program and the Legal Risk Management Certificate Program, which she helped develop. She has published articles on a variety of legal matters for the National Center for State Courts and the Aerospace and Defense Forum. She is affiliated with several professional organizations and institutions, including the Orange County Chapter of NCMA, the World Trade Center-San Diego, PMI-OC, OCRIMS, CPCU, Orange County Paralegal Association, Concordia University Irvine as an adjunct professor, Chapman University's eVillage, Irvine Valley College, and the Native American Procurement Forum. She is an active member of the State Bar of California and is admitted to the U.S. District Court, Central District of California.

Send comments about this article to cm@ncmahq.org.

ENDNOTES

1. Margaret Rumbaugh, *et al.*, *Contract Management Body of Knowledge* (*CMBOK*), fourth ed. (Ashburn, VA: NCMA, 2013): 15.
2. *Ibid.*

3. U.S. Sentencing Commission, *Guidelines Manual* (November, 2013).
4. Rumbaugh, *see* note 1, at 15.
5. *See, e.g.*, Jaeger, "Are Firms Lacking in Supply Chain Management?" *Compliance Week* (November 2013). This article discusses that companies have begun by investing in managing and monitoring business partners' compliance, just as is done with product quality. Yet, compliance officers for many companies still lack the support from senior management needed, which is why the article suggests that compliance officers find better ways to persuade to demonstrate how compliance can improve business operations in general.
6. *See, e.g.*, Lorenz Kahler, "Contract Management Duties as a New Regulatory Device," *available at* **http://lcp.law.duke.edu**. Essentially, the conclusion is that "how one manages contracts is not merely a business decision. Besides, even without the interference of the legislator, contract law might adapt itself to changes and develop new standards of care, such as a duty to establish a risk-management system."
7. *See* Virginia A. Suveiu, "Contract Risk Management to Survive and Thrive in the 21st Century," *Contract Management* Magazine (May 2015).
8. *See e.g.*, Dr. Andrea Bonime-Blanc, *The Reputation Risk Handbook*.
9. *See* Richard Epstein, *Design for Liberty: Private Property, Public Administration, and the Rule of Law* (2011), describing how corporations facing compliance issues are placed at mercy of their regulators rather than as equal adversaries.
10. *See, e.g.*, Geoffrey Miller, *The Law of Governance, Risk Management, and Compliance* (2014).
11. *See, e.g.*, Anthony Tarantino, *Governance, Risk, and Compliance Handbook* (2008).
12. For a general discussion on policies and programs, *see* Miriam Baer, "Governing Corporate Compliance," *Boston College Law Review* (2009).
13. *See* **www.ussc.gov/sites/default/files/pdf/about/overview/Overview_Federal_Sentencing_Guidelines.pdf**. For a broader discussion on privatization of compliance, *see* Scott Killingsworth, "The Privatization of Compliance," RAND Symposium, Transforming Compliance (May 2014).
14. *Ibid.*, at 1.
15. This is usually done in attempts to avoid triggering negotiation of customary contractual exceptions and protections. For more on this subject, *see generally* Dr. Andrea Bonime-Blanc, *The Reputation Risk Handbook*.
16. COSO is an umbrella of organizations in the fields of accounting, auditing, and financial management (*see* **www.coso.org**).
17. Committee of Sponsoring Organizations of the Treadway Commission, Internal Control-Integrated Framework (2013).
18. *See, e.g.*, Gov. Susan Schmidt Bies, "Remarks at the Enterprise Risk Management Roundtable," North Carolina State University, Raleigh, North Carolina (April 28, 2006), "A Bank Supervisor's Perspective on Enterprise Risk Management."
19. "Board Oversight of Management's Risk Appetite and Tolerance," *Harvard Business Review*, *available at* **http://blogs.law.harvard.edu/corpgov/2012/12/17/board-oversight-of-managements-risk-appetite-and-tolerance/#more-37330**.
20. This is so given that contract management, as a profession, impacts several areas within an organization, significantly influencing the organization's budget, operations, service, and reputation. For a general discussion, *see* chapter 1 of the *CMBOK*.
21. Again, it all goes back to the interrelationships of the contract manager (*see* Figure 4 at the end of chapter 2 of the *CMBOK*). The contract manager affects a wide circle.
22. In certain industries, such as the pipeline industry, those in the contract management profession do not deal directly with federal agencies (such as EPA or FERC). However, contract management professionals can still provide a risk management function for their entity. For example, the DOT 49 CFR Part 40 describes required procedures for conducting workplace drug and alcohol testing for the federally regulated transportation industry. Thus, contract management professionals can ensure that when preparing the contracts, the companies are advised of and comply with those specified procedures.
23. *See, e.g.*, the recent matter of United Parcel Service (UPS) where it agreed to pay $25 million to resolve allegations it violated the False Claims Act by submitting false claims to the federal government concerning delivery of Next Day overnight packages. According to the government, UPS engaged in multiple practices to conceal its failure to comply with its delivery guarantees, thus depriving federal customers of the ability to request refunds for late deliveries. The government's allegations arose out of a whistleblower lawsuit filed by a former UPS employee under the *qui tam* provisions of the False Claims Act. That former employee will receive $3.75 million as a result. For further information, *see* **www.justice.gov/opa/pr/united-parcel-service-agrees-settle-alleged-false-claims-act-violations**.
24. For instance, the Federal Energy Regulatory Commission (FERC)'s first Enforcement Policy Statement, adopted in 2005, encourages regulated entities to have comprehensive compliance programs to develop a culture of compliance within their entities, and to self-report and cooperate with FERC in the event of violations. (Enforcement of Statutes, Orders, Rules, and Regulations, 113 FERC paragraph 61,068 (2005).
25. Note that federal prosecutors undertake a similar analysis. Thus, if a potential defendant has operated a compliance program and has cooperated wholeheartedly with the investigation, such factors will count in the decision whether or not to charge that entity.
26. This also includes waiving of 75 percent of penalties for violations that were detected, reported, and remedied *without* such a compliance program in place. For more information, *see* **www2.epa.gov/enforcement**.
27. Since both are private agreements without a formal finding of liability, they do *not* involve judicial oversight. For more information, see Christopher J. Christie and Robert M. Hanna, "A Push Down the Road of Good Corporate Citizenship: The Deferred Prosecution Agreement Between the US Attorney for the District of New Jersey and Bristol-Myers Squibb Co.," *American Criminal Law Review* (2006).
28. Essentially, this makes boards more accountable. For a general discussion, see Betsy Berkhemer-Credaire, *The Board Game: How Smart Women Become Corporate Directors* (Angel City Press, 2013).
29. For example, see Delaware General Corporation Law section 114(a).
30. *See, e.g.*, *In the Matter of Steven A. Cohen*, SEC Administrative Proceeding No. 3-15382 (2013). The SEC said that Mr. Cohen failed to supervise two of his top traders, who were convicted of insider trading in 2013.
31. In *In re Caremark International Inc. Derivative Litigation*, the Delaware Chancery Court confirmed a board's fiduciary duty to oversee a corporate compliance program.
32. For instance, section 404(a) of Sarbanes-Oxley (15 U.S.C. 7262) requires that a reporting firm's annual report must contain an internal control report that provides for "the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting."
33. Contract managers play a multitude of roles along with reading and knowing all parts of the contract. In fact, seeing the entire contract, not just pieces or certain *Federal Acquisition Regulation* clauses, make the contract manager even more valuable from a risk management standpoint.
34. For detailed analysis of internal corporate compliance, *see* Bruce A. Green & Ellen Podgor, "Unregulated Internal Investigations: Achieving Fairness for Corporate Constituents," *Boston College Law Review* (2013).
35. *See* Rumbaugh, note 1, at 6.
36. For example, the government contracting world saw new ethics and compliance requirements via the Contract Code of Business Ethics and Conduct (48 CFR 52.203-13).