August 5, 2009

Effective Corporate Compliance Programs

By Ronald Kral, CPA, CMA, CGMA
Managing Partner of Candela Solutions LLC

We are living in an era of increased regulation and renewed enforcement efforts, especially for public companies as well as private companies in industries associated with the 2008 meltdown. Governmental regulation and enforcement is typically reactionary in nature rather than proactive. Could you imagine where we would be today if the mortgage origination industry and mortgage-backed securities had been regulated this decade? Obviously there are costs associated with regulatory compliance and I am not suggesting that everything needs to be regulated to a high degree. What I am suggesting is that it is in every organization's best interest to take seriously the need for a robust corporate compliance program.

The benefits of a strong program go well beyond regulatory and legal compliance to also include operational benefits. A well-balanced corporate compliance program will help ensure that a company's organizational structure, people, processes and technology are working in harmony to manage risks, keep customers happy, grow the business, oversee vendors, and achieve numerous other goals. Perhaps many of the recent company disasters could have been diverted with a robust program. It is always easier to look back on history and play "arm-chair-quarterback", but the beauty of a strong program is that it is proactive to divert failures and realize success. This article identifies several elements of successful corporate compliance programs, but first let's define a program and look at compliance within the realm of the bigger governance, risk and compliance (GRC) picture.

What is a Corporate Compliance Program?

A corporate compliance program is generally defined as a formal program specifying an organization's policies, procedures, and actions within a process to help prevent and detect violations of laws and regulations. It goes beyond a corporate code-of-conduct since it is an operational program, not simply a code of expected ethical behavior. Clearly, a code-of-conduct is an important component of a compliance program and ethics remains the heart and soul of all corporate compliance programs. However, a comprehensive program goes further by applying the code to the specific risks of an organization and integrating measures to address those risks.

Some companies think of a corporate compliance program as strictly addressing external regulatory considerations. A more integrated approach also focuses on legal as well as internal compliance to mitigate the risks of fraud, as well as to reach strategic, operational, and financial reporting objectives. Think of a corporate compliance program as a magnet that brings all of a company's compliance efforts together. It is essentially a codification of applicable regulatory and internal compliance requirements, as well as a roadmap to action. A comprehensive program helps position a company to divert disasters, meet objectives, and grow shareholder value.

Many organizations have components of a program in place. However, the question that must be asked is; are the components collectively maximizing organizational value or wasting resources through

duplicative efforts? A company with bits and pieces of a program organizationally scattered, and operating in a complex environment, is greatly challenged from a cost-efficiency and effectiveness standpoint. Oftentimes regulatory processes are siloed leading to a host of inefficiencies. While enterprise software can go a long ways towards addressing these inefficiencies, it often comes down to the organizational and cultural considerations to ensure an effective program across all significant risk areas. For example, those companies who have walked down the Sarbanes-Oxley (SOX) road may have extensive policies, procedures, and testing to assess the effectiveness of entity-level controls; however, are these efforts properly integrated with those of FCPA, labor laws, PCI, etc.? Oftentimes, documentation and testing efforts can be used for multiple legal requirements and company objectives, especially in the areas of entity-level and general IT controls.

Keep it Focused and Simple to Help Ensure Adherence

The more complex, the more difficult it is to communicate a corporate compliance program to employees and stakeholder groups. Consultants and professional trade organizations have a field-day with all sorts of approaches, frameworks, and models on compliance programs. This occurs because of semantics, multiple variables, and the inter-related disciplines of compliance. Compliance goes hand-in-hand with governance and risk management, otherwise known as GRC. It is very difficult to successfully isolate one without considering the other two. For purposes of this article, let's focus on the "C" in GRC, but as you will read this is not entirely possible since all three areas are highly interwoven in concept and practice. This occurs because each element of governance, risk and compliance encompasses organizational factors, people, processes and technologies that cannot, and should not, be viewed separately. With this in mind, let's proceed knowing that governance and risk management are deeply imbedded in any effective corporate compliance program.

Ten Considerations to Help Ensure Effectiveness

There are certainly many ingredients and aspects to an effective corporate compliance program. One excellent source of information is Chapter 8, Part B, entitled *Remedying Harm from Criminal Conduct, and Effective Compliance and Ethics Program* from the United States Sentencing Commission. These Federal Sentencing Guidelines forward a minimum set of requirements for development of an effective program to prevent and detect violations of law.

Here are some aspects that go into the making of an effective corporate compliance program. This list of ten considerations can be used as a checklist to see where your organization stands:

1. **Understand the Scope**: Identify all regulatory and internal compliance needs and efforts to challenge if organizational responsibilities are properly aligned. This should not be a "one and done" step, but rather performed periodically as regulatory landscapes and operational environments are typically changing. You need to address this one in tandem with the next three.

2. **Gather Internal and External Intelligence**: Tap into the collective intelligence of your company by soliciting thoughts from the Board, management and employees. Also look beyond the walls of the organization to understand industry developments and competitor reactions to corporate compliance. This includes researching legal actions to help identify risks.

3. **Define Objectives**: Define objectives (things to accomplish in order to achieve a goal) from an enterprise and business unit standpoints. This should be a significant part of the periodic strategic planning process.

4. **Conduct a Risk Assessmen**t: Identify risks, probabilities, and the significance in terms of both

qualitative and quantitative measures. Consider scenarios from a cause-and-effect standpoint.

5. **Align Controls**: Policies, procedures, and actions within a process, should be in place to address the risks to best achieve objectives.

6. **Verify Buy-In and Understandability**: Everyone needs to know their roles. For control owners to be expected to act appropriately, they need to understand the "why" and "how" of the compliance program. Controls need to be clearly communicated, ideally with a feedback loop so control owners can voice their insights and concerns.

7. **Test Cultural Support**: Many organizations have put in place paper programs that have no real effect on the operations of the organization. Determine if the cultures at headquarters and all relevant business units are supportive of a strong corporate compliance program. This can be accomplished through surveys, independent reviews and entity-level control assessments.

8. **Assess On-Going Compliance**: Build monitoring, internal audit and special reviews into the compliance program to help ensure that controls are operating effectively. This effort should also seek to identify the most-efficient alignment of responsibilities and controls.

9. **Train, Educate and Communicate**: Deliver periodic targeted training and share compliance information with the business units, global functions, external partners, customers, vendors, and other stakeholder groups.

10. **Measure Results and Report to Board**: Develop a reporting dashboard to keep management groups and the Board aware of compliance measures, trends and developments. This should address both internal and external activities.

Each and every one of the above considerations should be built into the corporate compliance program. If your answer was not affirmative to any of these items, chances are you have plenty of opportunity to make your compliance program more efficient and effective. A lapse in anyone of the above ten areas could spell "doom" for your compliance efforts. Don't think of compliance as simply a regulatory necessity, but rather as a means in protecting your number one asset – your company's reputation.

*****

Ron Kral is the Managing Partner of Candela Solutions LLC, a public accounting firm with a national focus on governance, SEC compliance, and internal auditing. He is an educator, advisor, and internal auditor for boards and management teams. Ron is a member of 4 of the 5 COSO sponsoring organizations; the AICPA, FEI, IIA, and IMA. He can be reached at rkral@CandelaSolutions.com.

Candela Solutions LLC is a strategic CPA firm in providing services to US public companies that external auditors cannot due to independence concerns. Visit our website at www.CandelaSolutions.com

This is an article reprint from the Governance Issues™ Newsletter, Volume 2009, Number 4, published on August 5, 2009