Compliance & Ethics Professional

May/June 2013

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

www.corporatecompliance.org

Meet Michael Miller

Executive Director for Ethics and Compliance, Aerojet, Sacramento, CA

See page 14

by C. J. Rathbun, CCEP, FLMI, HIA, AIRC, ACS

You've identified a corporate risk—what next?

» The company's choices in response to an identified risk will depend on its risk tolerance.
» The CCO's considerations should include how mitigating the risk will affect everyone from the board room to the mailroom.
» The CCO's report should be carefully designed for its target audience.
» Internal procedures may need to be changed to prevent future risks.
» Proactive monitoring and/or auditing will help you catch problems before they become issues.

The scope of risk management extends all the way from the boardroom to the mailroom. The overall impact to the organization, though, is first addressed at the management level by the chief compliance officer (CCO). Once the board or chief executive officer has determined how the company will address any specific risk, much of the planning and implementation responsibility falls back on the CCO's shoulders.


Rathbun

After your company identifies a risk, management will consider at least these three dynamics before making its choice of actions.

1. The severity of the risk weighed against the company's appetite for risk.
2. How the company has performed in the past on managing similar risks and if so, what the impact might be on the company if the risk actually occurred.
3. The probability or likelihood of the risk event occurring.

Shaping the compliance report

What considerations, then, should go into preparing your compliance officer's report to the decision-making group on this newly-identified risk? The report should be shaped by answers to the following questions.

- **Who is the audience**? Is it the board of directors? The CEO? Or does it begin with other C-suite executives? What is the trust level that has been established with that audience? Sometimes the audience may even be the regulatory body that previously examined your organization and wants you to provide a follow-up report.
- **What is the organizational culture?** How is a decision of this dimension usually made? How much detail does the audience expect? What stories or examples will illustrate it best?
- **What reputational risk for the company should be anticipated?** Would the company be comfortable with this decision being published in *The Wall Street Journal*, for instance?
- **What should be incorporated into the report?** What other business concerns, financial pressures, and legal liabilities will it include?
- **How should the report be presented?** In what format or with what technology? Although this factor may seem a less important consideration than the others, it will become increasingly more important as generations in the board room and C-suite change.

The compliance officer's recommendations for action may rest, in large part, on what the company can bring to the table to successfully support the decision. This accounting should permeate all impacted stakeholders of the company, from the CEO to mailroom employees, and from board member to vendor representatives. Critical factors to consider in these positions are acceptance of or resistance to change, necessary skill sets, and the extent of employee buy-in to the cultural norms and corporate values.

The compliance officer's recommendations for action may rest, in large part, on what the company can bring to the table to successfully support the decision.

Weighing the options

As a result of the compliance officer's report and recommendations, the ensuing discussion will result in a decision outlining the desired course of action.

That course of action will fall into one of four categories. First, if the company's responses to each of the three factors listed at the beginning (severity, performance, and probability) result in a negative "score" (i.e, high risk/low tolerance, not well-managed, and high likelihood), the company may choose avoidance—getting out of the risk-bearing activity completely. For instance, if new legislation makes a non-core product much more risky in terms of required monitoring or increased regulatory scrutiny, and the company is historically conservative, the severity factor is a "red light."

If the company does not already have a strong infrastructure for monitoring and/or field supervision, or is simply too small to have the resources for managing the risk, the impact of an occurrence could spell trouble for the company—another red light. So the company must also determine what the likelihood is of that occurrence. If the perception that there is a high possibility of an event, along with the red lights on the severity and performance factors, the company may well want to withdraw from the market.

Secondly, in the same scenario of a regulatory change in a non-core line of business, the company may determine to make changes to their field or internal monitoring that will potentially: (a) reduce the severity of risk, (b) improve their performance score on this risk with careful management, and (c) hope that the event will not happen on their watch.

Another choice common in the insurance industry is that of allocating or transferring a portion of the financial risk to those who specialize in accepting that transfer. And the fourth choice, of course, is to accept the risk and the potential for financial impact, believing that current protection protocols will be adequate in the face of the newly-identified risk. This choice is generally made because the company's cost-benefit analysis supports the position that the potential gain, when balanced against potential problems or loss, is perceived to be worth the gamble.

Implementing the company choice

The second choice (making changes to address or minimize the risk) is the one that involves the most effort and change, a large portion of which lies in revising your internal procedures in order to help manage the risk best. Your current compliance structure should

include the protocols you need in order to explore the ripple effect within the company when it has made this decision. Once the potentially affected departments, business units, operational functions, and outside stakeholders are identified, the work of making appropriate changes to policies, procedures, and actual behaviors begins.

What behaviors will demonstrate compliance with this decision? Each impacted employee position should be considered, as well as actions of the officers, producers, vendors, and even possibly board members. What factors in that behavior are measurable and how are they quantifiable? Short-term, mid-term, and long-term behavior measurements should be incorporated into the answers. Depending on the magnitude of the risk potential, what disciplinary actions ought to be incorporated into the protocols? What deterrent actions is the company legally and ethically prepared to take across all stakeholder levels?

Designing the policies and procedures will take time. The support needed to successfully navigate this risk may require significant changes to some employees' daily actions. Training and implementation—if you truly imbed the new procedures into the workaday lives of your employees—could also take some time.

Once that process is well on its way, compliance with and effectiveness of the new activities will need to be determined. How will the company help ensure that those changes to behaviors stay in place? Employee engagement and accountability should be included in that oversight. How will the activities themselves or the effectiveness of those activities be checked after they are instituted?

Confirming the changes in behavior

The two basic ways to structure "check-back" functions on procedures, actions, and accountability are ongoing monitoring or an after-the-fact audit (meaning operational assessments, rather than financial). Some changes may call for an even more intensive structure, a combined approach of both ongoing and regular monitoring, and regular follow-up assessments. The use of these tools may begin on a heightened schedule, but the frequency can be lowered as consistent completion of procedures and the reliability of their outcomes builds more confidence internally.

A note of caution, however. As familiarity with the procedures grows, the effectiveness of monitoring and/or auditing may weaken. Two factors could be at work here. One is that the monitoring may become less rigorous because of the level of confidence reached. Second, as procedures continue to grow and change, the assessments may not stay in step with those changes and may become less effective.

Some changes may call for an even more intensive structure, a combined approach of both ongoing and regular monitoring, and regular follow-up assessments.

Which of the two confirmation methods you select can depend on those three initial factors mentioned above: the severity, management capability, and likelihood of the risk. It can also be influenced by the regulatory and hierarchal structure of the company, the number of employees and resources available, and the methodologies already in use for similar risks. For instance, if regular, quarterly

compliance audits are already done in the areas impacted by the new procedures, it is relatively simple to add a new review section to the existing procedure. However, if your staff is few in number and typically works more with trend analysis and measurement reporting, you are more likely to use those monitoring methods.

Other familiar monitoring tools include affirmation of training, attestation of compliance by vendors and producers, gauging knowledge levels of employees and producers, quantifying completion and accuracy rates, and evaluating increases in complaints or hotline calls about an impacted area. Some less familiar tools which appear to be gaining traction in the ethics and compliance community are:

- Monitoring and listening to communications of employees on social media blogs, Facebook, and Twitter. This should not be done with punitive mind-set.
- Early identification of "hot spot" events or statements.
- Stakeholder teleconference calls, town hall meetings, sales meetings.
- Employee and consumer focus groups.

The end goal of risk management

Having accepted the challenge of an identified risk, the company's well-structured program likely requires vigilance and encourages continuous improvement of both company procedures and of the monitoring and/or auditing of those procedures. One of the prime objectives of designing such a proactive system is to allow the company to identify a growing concern before it becomes an issue—and before consumers are harmed or regulators become concerned. Your goal is to help ensure that you and your company will "get the first crack" at addressing a problem, if one occurs. ✳

C. J. Rathbun *(cj.rathbun@firstconsulting.com) is Senior Consultant with First Consulting & Administration, Inc. in Kansas City, MO.*