Getting Governance Right:

A Handbook for Today's CEO and the Board of Directors

CORPORATE COMPLIANCE INSIGHTS

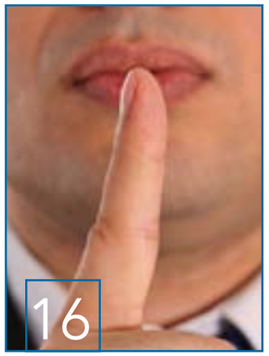
Getting Governance Right: A Handbook for Today's CEO and the Board of Directors

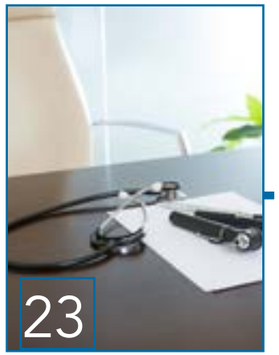
PUBLISHER
Maurice Gilbert
maurice@corporatecomplianceinsights.com

MANAGING EDITOR
Sarah Normand
sarah@corporatecomplianceinsights.com

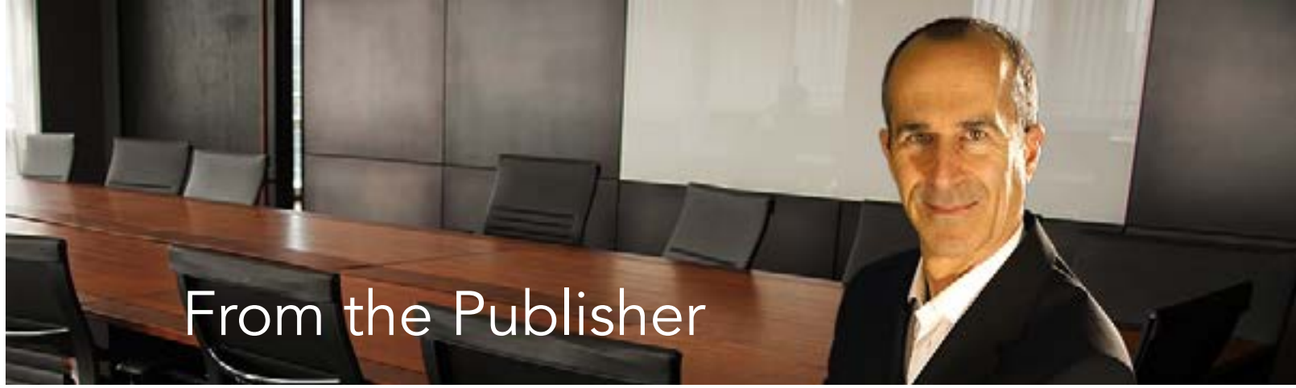
EDITOR
Emily Ellis
emily@corporatecomplianceinsights.com

TABLE OF CONTENTS





FEATURES



From the Publisher

Corporate governance has been the focus of regulators' attention of late, and the performance of the Board of Directors is increasingly integral to an organization's success in the marketplace. It's no wonder, then, that companies are striving to enhance their governance practices and position their Boards to excel.

This book brings together expertise on all things Board related, exploring topics from best practices to the benefit of diversity and the Board's role in reducing risk and improving cybersecurity. In this comprehensive guide, our expert authors explore the top issues plaguing Boards and prescribe actionable solutions. You'll find no platitudes here. Nor do we avoid the uncomfortable topics.

CCI is proud to feature thought leadership from some of the greatest minds in the governance, risk management and compliance field, so we're pleased to present this work, a compendium on Boards.

Maurice Gilbert | CEO, Corporate Compliance Insights

CORPORATE COMPLIANCE INSIGHTS

10 Ways for CEOs to Improve Corporate Governance

LINDA HENMAN

In order to achieve maximally effective governance, CEOs and Boards of Directors must work hand in hand. A governance committee can be helpful in fostering this partnership, but with or without governance committees, CEOs must take an active role in improving Board performance. Linda Henman offers 10 strategies to do just that.

In parts of Indonesia, Komodo Dragons make unwelcome and unannounced visits to villages that border their habitat. Even though the giant lizards and humans lived in harmony for generations, contention exists now because environmentalists have imposed new policies in a region where people perceived a sacred duty in caring for the Komodo Dragons. The relationship between lizard and human has not been the same since.

External forces have imposed new regulations on Boards too, causing CEOs and directors to experience a similar loss of symbiosis.

Now, more than ever, directors are taking their responsibilities seriously, speaking up and striving for results; but in many cases, the evolving relationship between the CEO and the Board has not found the right symmetry. Discovering it will depend on several factors, with improved corporate governance leading the way.

"Governance" is one of those all-encompassing words that people use, but that few can explain in concrete terms. The dictionary defines governance as supremacy, domination, power or authority. People in corporations usually use it to mean general Board oversight.

Governance underpins the Board's ability to do all the aspects of its job. While strategy and succession planning address specific "what" questions, governance deals with the "how." It includes, but is not limited to, decisions about the Board's size, frequency of meetings, director selection, shareholder relations and social responsibility. When a Board has a governance committee, those directors initiate action plans with specific timelines for implementation of recommendations. This committee should have the authority to shape and recommend policy and structure.

The existence of a governance committee doesn't let the CEO off the hook, however. To improve overall Board performance, CEOs need to play an active role in how things happen. Here are 10 ways to do that:

1. Formulate strategy for the Board's critique, and have strategy drive the agenda. Effective Board governance involves assessing strategy, not setting it. Therefore, the more the CEO does to articulate the strategic direction and clarify the measurements, criteria, timelines and standards for evaluating it, the more likely the Board will be to offer oversight of its progress.

2. Tackle important, difficult and unpleasant issues immediately after the meeting starts. If you wait several hours, everyone will be tired and impatient. You'll get a better caliber of discussion earlier in the day, and the energy will be higher once you've made the tough calls.

3. Most Boards hold executive session meetings following the Board meeting. Once again, if the meeting occurs late in the day, people will be spent. You can benefit, therefore, from an "executive session sandwich." In other words, meet before the general meeting to address critical issues and then use the low-energy time after the session to tie up loose ends.

4. Use the Board book to inform, not persuade. If the book includes mountains of data with little salient information, directors will overlook key issues. Lead with a summary page, the questions you'd want to discuss and the topics that merit debate. In short, discuss, don't present the book. Whenever possible, enrich committee reports too. Typically, these reports include a detailed description that lacks relevant information or that rehashes an entire committee meeting or topic. Aggregate the critical information; present it in summary form; and offer analysis, not just information.

5. Avoid death by PowerPoint. Too often the slide presentation offers little more than the book in electronic format, and the presentation eats up valuable meeting time. Dialogue, not more slides, holds the key.

6. Encourage directors to communicate regularly about their experience and expertise. You should know how to pull this from the directors when you need it, but if you have never formally gathered this information, it won't exist in a time of emergency or decision making.

> "'Governance' is one of those all-encompassing words that people use but that few can explain in concrete terms."

7. Play an active role in the selection of new directors, and work closely with the governance committee to choose the best and brightest that will bring diversity of thought to your Board.

8. Unless you are the chair, evaluating the Board won't be your primary responsibility, but you can still drive it. Encourage evaluations of directors. Have a clear, agreed-upon purpose for evaluations. Do you want to improve overall performance? Individual performance? Drive shareholder value? Eliminate someone from the Board? In a confidential format, have directors evaluate peers based on observable behavior that highlights how this person can add more value. Then, provide private feedback to each director, preferably delivered by a third party. All records should be "paper and pencil" so they can be shredded. Include an assessment of committees, too. What is the quality of their reports? Are they transparent? What is the overall relationship to the Board? Does the committee drive shareholder value? When using a survey, customize it to your needs. Measure only those categories that are directly applicable.

9. Routinely evaluate the composition of the Board, not just the performance of the directors. As the direction and strategy of the organization shift, so should the skills and experiences of the directors.

10. Ask the Board to conduct separate evaluations of key executives at least once a year, but seek timely feedback in executive sessions or private conversations. Above all, don't create materials that can be subpoenaed. Request a Board evaluation of yourself. Ask for feedback about these:

- *Recruitment of top talent*
- *Development of executive team*
- *Allocation of the company's resources*
- *Role modeling of effective leadership*
- *I mplementation of long-term strategies to maximize opportunities and mitigate risks.*
- *Acting as the chief spokesperson for the company*
- *Effective communication with shareholders and all stakeholders*
- *Communication with the members of the Board of Directors*

Active, compliant Boards and CEOs no longer offer organizations enough. Companies need and demand stellar performance from both individual contributors and the Board as a whole. Your success and that of the organization depend on your taking a more dynamic role in finding symmetry and symbiosis for all concerned.

Linda Henman
Henman Performance Group

The Board of Directors and Compliance: Four Ideas for Improving Effectiveness & Reducing Risk

STUART ALTMAN

A number of high profile corporate scandals at some large and supposedly sophisticated companies have, if nothing else, driven home the fact that no matter how strong you think your corporate compliance and ethics program is, the risk of failure is still there.

A number of high-profile corporate scandals at some large and supposedly sophisticated companies have, if nothing else, driven home the fact that no matter how strong you think your corporate compliance and ethics program is, the risk of failure is still there. Let's look at this issue from the standpoint of the Board of Directors.

Right now, there are a number of very concerned directors asking themselves whether they have done all they could, or should, have to prevent this and what are the ongoing risks, not only to the company, but to them personally. True, directors should always be thinking about the institutional risk to the company, but nothing motivates effectiveness like the risk of personal liability.

Ordinarily directors are protected by the business judgment rule, which provides that well-informed decisions of directors taken after due consideration and in good faith will not be attacked by a court because the decisions turned out wrong. In cases of compliance failures – whether issues of foreign bribery, cartel activity or environmental hazards, to name a few – the issue for a Board is usually one of omission. Rarely has a Board approved such activity. Rather, the issue is whether it has done everything possible to avoid such conduct. Here are four ideas that can help strengthen the effectiveness of the Board in these situations and thus, limit risk.

1 TRAINING

Interestingly, in many companies directors do not necessarily receive the same compliance training that employees do. Directors may claim they are too constrained by time, or that they, of course, know this material already. Perhaps they do, but even if the directors are compliance experts, shouldn't they know how the employees are trained? How do you measure the effectiveness of a program you have opted out of? In short, directors should go through, at a minimum, the same training employees receive. But that is not enough. Directors need specialized training, not just in the nuts and bolts that line employees receive, but also in the issues at the center of compliance and ethics. Directors need to be focused on the big picture of why a company has a compliance program. They need to know what questions their compliance professionals should be asking, and if directors don't see this happening, they need to act quickly.

Moreover, at least some of this training should be external to the company. Even if management is well intentioned, it is vital that directors get an occasional different perspective on compliance from that which prevails in the company.

2 STRUCTURE

A long discourse of the various pros and cons of possible compliance structures would fill several of these columns. There is an active professional debate out there as to whether or not the Chief Compliance Officer should be separate from the General Counsel. Should both ethics and compliance roles be rolled into one position? Where does internal audit fit in? I won't attempt to evaluate these debates here. Indeed, there may be no one right answer. But the way in which your company structures these roles is vital to your governance and your ability to address compliance and ethics.

Boards of Directors should be intimately involved in planning for these issues. Directors should regularly review the existing structure and make sure they are comfortable with it and it is serving the company's interests. Whatever the specific structure chosen, those primarily responsible for compliance must have direct access to the Board or a compliance committee. Given this dictate, you can decide what works for your company. Is your organization hierarchical in nature? Are managers expected to closely follow superiors with little questioning? If so, asking a GC who reports directly to the CEO to also serve as CCO and report to the Board may place him or her in an unworkable position. If the CFO uses internal audit as a personal resource, how comfortable can the Board be that the head of IA would bypass that CFO if the situation called for it? On the other hand, where a company operates in a matrix environment with multiple reporting lines standard, such dual roles and reporting may come naturally.

3 SEEK ADVICE

Most Boards of Directors do not have separate counsel from the entity they serve. Directors typically rely on the General Counsel and regular outside counsel to do their job except in the rare situation such as the need for a special committee and counsel thereto. In general, most Boards do not need regular and continuing counsel involved in every decision they make. But that does not mean such outside advice may not be useful some of the time.

Every Board should have a relationship with counsel independent of the company and its management -- someone who can be called upon in those rare times when the directors feel that they need a truly independent voice. Directors need to avoid making this counsel into a crutch on which to lean any time they need validation or have a tough decision to make. But at the same time, they need to be willing to seek outside advice when the situation demands. Setting up this relationship in advance makes that all the easier.

4 EVALUATE

Evaluation of the efficiency of a compliance program is commonplace. The CCO does it. IA plays a role. Board members weigh in regularly. But who evaluates whether the Board is doing its job when it comes to compliance? Company officers are unlikely to risk angering the Board by criticizing their work in this area. Often, the only judgment comes when there has been a compliance failure and the inevitable derivative action.

Instead of waiting for disaster and trial by fire, Boards should consider bringing in a consultant to work with them in evaluating how they fulfill their compliance and oversight role. This should be something the Board does for itself and can be combined with the training discussed above. Whether the evaluator be an outside law firm or one of the many consultants available in the compliance field, an outside voice can be a great check on the natural tendency to overestimate our own effectiveness.

The Board of Directors has a difficult role in this area. They need to protect the company and themselves. These four steps will make that job easier and make them more effective.

Stuart Altman
Hogan Lovells US LLP

Corporate Governance: Five "Worst Practices"

DAN HURSON

Dan Hurson, in a somewhat contrarian spirit, presents his shortlist of "worst practices" in corporate governance and compliance.

In the ever-expanding universe of corporate governance and compliance, we are constantly reading of "best practices" recommended by one expert or another. They tend to be somewhat sterile, repetitious and obvious. A book full of such insights, while important, can be a very dull read.

It is certainly true that company executives or managers who zealously follow "best" practices will become better at their jobs and help their companies, and if properly documented by those individuals, such sterling habits can promote bonuses and career advancement. We are not here to denigrate that which has been declared "best."

But let's be honest: it's much more interesting to read about the seemingly endless number of screw-ups, misfeasance, malfeasance, scandal and downright stupidity that has in recent years characterized many corporate actions. How did they make such errors, we ponder, and are amazed at what they failed to see coming and how badly they handled it once it hit. Depending on how honest we are with ourselves, our reaction is usually either "I would never make such a mistake" or "there but for the grace of God go I."

In that somewhat contrarian spirit, I present my shortlist of "worst practices" in corporate governance and compliance. My list is not exclusive by any means and may reflect heavily on my background as a lawyer, with prior prosecutorial stints with the DOJ and SEC, and as an in-house lawyer for a large public company. After reading mine, I encourage you to write one for yourself, draw upon your own experiences, and be honest. In the process, take a hard look at your own company and the challenges and risks it faces today, and see if you can't identify a "worst practice" or two in your organization. Here's my list:

1 Always Believing "The Smartest Guys in the Room"

In business, as in life, we are constantly reminded that there is always someone around who is just plain smarter, more articulate or more successful than we are. Often they are better looking too, which will usually explain everything. Those types generally seem to know it, live it, profit from it and probably flaunt it.

In the business world, they often become CEO's, influential Board members, rising stars, consultants, experts, gurus and in general exporters of influence and advice. Many corporations retain them, promote them and routinely follow their advice. Sometimes they are viewed as comers and you just want to be on their team. Sometimes they are hired to provide bulletproof CYA insurance for management and Boards of Directors.

"...it's much more interesting to read about the seemingly endless number of screw-ups, misfeasance, malfeasance, scandal and downright stupidity..."

Painful as it may be, they are sometimes right (maybe some of them really are smarter) and should be followed. But sometimes they are wrong, and companies follow them right down the path to terrible consequences.

How many times have you been in a meeting, read a report or otherwise had to defer to the supposed wisdom from such folks and felt like saying "that's just a bunch of [supply expletive]?" You seen wide-eyed board members misled, confused or bowled over by such folks with presentations and reports which you know are misleading, self-aggrandizing or just flat wrong. How often has your company hired expensive supposed experts to tell it something that sounds impressive but just doesn't sit well with you? You firmly believe you know more than they do, and want to speak up or reply, but you are intimidated, unsure or unwilling to stick your neck out. Just like in grade school, the safe route is to keep silent, don't raise your hand -- and see which way the wind blows.

How many recent corporate governance disasters can trace their origins to such dumb acts of personal timidity and self-preservation? How many smart people in so many places knew that home loans were being made to people who could not or would not repay them? We all know now how such selfish "head in the sand" avoidance cumulatively led to an enormous, worldwide financial disaster which almost certainly could have been avoided.

Most recently, how many smart engineers, technicians or scientists knew there was something wrong on the BP drilling platform, or more broadly knew the company (or the industry) had not sufficiently anticipated, quantified or prepared for the risks of deep water drilling, but chose not to speak up?

What is it at your company that's being driven by the "smart guys," or the hired guns, that you think is wrong-headed, misguided or just plain reckless? How long will you be content to stay silent? Being able to say "I should have told you so" is not very satisfying after your company fails -- or worse, kills someone. This attitude is my nominee for the first and perhaps most insidious, yet easiest avoided, of the worst practices.

Allowing Strategic Planning and Risk Management to Become Problem Avoidance

2

There are certain problems that stare us in the face, are not going away, and must be dealt with despite the near certainty of painful consequences if they are dealt with directly. For most problems in business, as for some -- but not all -- in life, there is usually a solution, however difficult. The "worst practice" is papering it over, studying it, deferring it or ignoring it. I call this "problem avoidance." I would venture to guess you are experiencing it right now in your company. Make an "honest" list just for yourself: column one, the problems; column two, how to fix them (in six words or less); column three, what is being done about it right now; column four, how you think it's going to come out.

If you find that your organization is doing nothing about the problem(s) on your list, you have a problem. Your company is reckless, stupid or both. If it is aware of the problem and is addressing it with some committees or outside consultants, waiting for some future event which may never happen or just waiting for the next fiscal year, you are probably already in trouble. Ditto if you identify good "fixes" that are not being implemented right now, have been deemed too expensive or have been studied before without resolution.

CONTINUED

If the "problem" is the presence in your organization of a toxic individual, how long before they do something very destructive? In short, what might look like a "best" practice, addressing a strategic issue in some deficient manner, may just be a "worst" practice—problem avoidance with no resolution in sight.

Denigrating, Underestimating or Infuriating Regulators

3 In a world in which the government has become such a pervasive regulator and overseer of every facet of business activity, it is astounding that so many otherwise smart, seemingly well-run organizations continually get themselves in trouble with the government. Some of these confrontations end quietly, with a reprimand or fine, maybe a one-day story in a trade publication. Others fester into full-blown disasters, involving at a minimum fines and bad publicity, and at the worst, criminal investigation and sometimes prosecution of individuals. Most end somewhere in between, but the result is never very good. Shareholder funds get spent needlessly, market value is diminished, reputations and careers are harmed and sometimes people, or the environment, are injured.

Upon closer examination, many of these situations need never have happened. Some companies and their management teams simply view their regulators as hacks who must be tolerated, and any time they can be thrown off the scent, misled or delayed in doing their jobs, is considered a victory. Sometimes the company tries to cooperate, explain or compromise, but falls short because someone is caught playing fast and loose with the regulators, which may consist of as little as dragging out responses to questions, misleading them on some seemingly minor matter, withholding documents in an investigation, taking an overly technical or legalistic position known to infuriate the government or making a dumb statement to the media (e.g. "I want my life back," Tony Hayward, BP, May 2010).

Sometimes the mistake is well-intentioned, and may for legal reasons be the most protective, but not in the context in which it is employed. For example, companies lately seem to be sending representatives to congressional hearings who are not well prepared, are personally clueless about how politicians function or are so over-lawyered and fearful of admission of some liability they can barely state their names. The auto execs who flew in to Washington on their private planes while looking for billions in handouts come to mind, as do the BP, Transocean, Halliburton trio of pathetic finger pointers dragged before congress in the Gulf oil spill debacle.

"Some companies and their managements simply view their regulators as hacks who must be tolerated."

These missteps have a common thread: lack of appreciation of the power of the government to react harshly, even if unpredictably, unreasonably or in error. The organization that plays around the margins with its regulators, or allows itself (rightly or wrongly) to be perceived as standing in the way of the regulator's inquiry, being less than totally transparent or of turning a deaf ear to the public interest (at least as seen by the regulator), is committing a "worst practice." Once done, it is hard to repair the damage.

Investigating, Documenting and then Ignoring Problems

4 We live in the golden age of the internal investigation. The government wants corporations to investigate themselves at the hint of any impropriety. Typically the investigation is done by a law or consulting firm and then turned over to the SEC, DOJ or whomever is the appropriate regulator. Credit is usually given for a full, prompt and honest report. Such reports, sometimes called internal evaluations, have in one form or another been done for years, even before they were routinely demanded by and given to the government. Boards of Directors and General Counsel like to have them written, even if they get filed away, to show they are doing their jobs.

While such reports and evaluations, together with the usual set of recommendations, are presumably read, discussed at high levels and some action may or may not be taken, the issues raised often persist, inadequately addressed, if addressed at all. Some investigations and reports, as time passes and personnel change, are more or less forgotten. A recent example is a report done by a law firm years ago for Wal- Mart.

The company, according to a recent New York Times article, had hired the firm "to examine its vulnerability" to a sex-discrimination suit. The 1995 report allegedly found "widespread gender disparities in pay and promotion at Wal-Mart and Sam's Club Stores." The lawyers are said to have concluded that without significant changes, Wal-Mart "would find it difficult to fashion a persuasive explanation for disproportionate employment patterns." Wal-Mart has now called the report "deeply flawed" and "stale."

Inevitably, a massive class action sex-discrimination suit was filed in 2001. The long-forgotten report was recently leaked and the class action lawyers, who have just achieved class certification after years of pre-trial motions, are trying to get their hands on it, despite the obvious initial obstacle of attorney-client privilege.

A similar paper trail may haunt BP as well. Pro Publica and the Washington Post have recently reported that BP had initiated "a series of internal investigations over the past decade [which] warned senior BP managers that the company repeatedly disregarded safety and environmental rules and risked a serious accident if it did not change its ways." Pro Publica concludes that the documents "portray a company that systematically ignored its own safety policies across its North American operations…" These internal reports will surely be on the exhibit lists for the endless congressional hearings and court cases that the company will face for years to come.

No good deed goes unpunished, so no good internal investigation should go unheeded. How many studies, reports, evaluations, critical emails, committee minutes, speeches, internal audit reports, external auditor management letters and similar time bombs are lying around your company? If you sat down with a good plaintiff's lawyer and he asked if each recommendation and warning in each report had been acted upon, how would your answer sound? Filing away internal reports and investigations for another day, or failing to address their recommendations in a demonstrably effective manner, is a worst practice which can boomerang anytime from here to eternity.

Failing to Make Your Outside Auditors Uncomfortable

5 Public companies generally pay handsomely for competent audit services, including the annual clean audit opinion and favorable opinions regarding internal controls. In the course of doing their work, outside auditors should be getting into many aspects of the company's internal controls, financial operations and, informally or otherwise, the personalities and practices of the company's top officers and managers.

Auditors learn things during their work that they do not always disclose to their clients. They are required, under GAAS standards, to conduct an annual "brainstorming" session with the members of the full audit team to assess the possibilities for fraud at the company. Even junior auditors are encouraged to speak up and discuss how fraud might develop, and who might be prone to engage in fraud. A memo of that meeting should be created, and it can make for fascinating reading. Likewise, when auditors decide to take on new clients or retain them for another year, they generally do risk assessments of the client, evaluating the odds that the company may engage in fraud.

Audit partners, who generally do most of the interface with the audit committee and top management, are generally loath to discuss these evaluations outside the audit firm (unless the firm concludes some obvious and serious issue exists), as they may cast aspersions, even indirectly, on top managers with whom the audit firm is most anxious to maintain good business relationships. Top management, and especially the CFO and audit committees, should press to see these SAS 99 memos and any internal audit documents reflecting potential fraud risks at the company, however speculative or hypothetical. They should also demand the right to separately question junior members of the audit team, who may be more candid with the audit committee. There are too many cases to count where the auditors knew something was wrong in time to avoid disaster but chose, for whatever reason, not to follow up and not to report it to the audit committee. Even if a company is very satisfied with its auditors and considers them competent and candid, there is no reason not to press them hard for any and all information about what may be concerning them and how they have quantified any concerns, for those observations should be concerning the Board as well.

Conclusion

This is my shortlist of "worst practices." More important is what is on your list. Indeed, your company should consider having every top manager make their own list and deliver it to some designated officer who can decide if action is needed. The successful corporate compliance program must be a proactive, aggressive and occasionally uncomfortable search for the worst, not just the best, practices.

Dan Hurson
Hurson Law

Five Risk Categories for Focusing the Board's Risk Oversight

JIM DELOACH

Many companies have adopted a risk language to facilitate dialogue within the organization regarding their risks. While we are not aware of an authoritative risk language or model, there are a number of risk models in the public domain that can be useful to ensure the completeness of the event categorization and risk assessment processes.

Many companies have adopted a risk language to facilitate dialogue within the organization regarding their risks. While we are not aware of an authoritative risk language or model, there are a number of risk models in the public domain that can be useful to ensure the completeness of the event categorization and risk assessment processes.

The central purpose of a common language is to avoid the problem of beginning a risk assessment with a blank sheet of paper with all of the start-up activity that entails. Simply stated, a common language enables busy people with diverse backgrounds and experience to communicate more effectively with each other and identify relevant issues more quickly regarding the sources of uncertainty in a business.

As the Board of Directors engages executive management in conjunction with exercising its risk oversight responsibilities, the question arises as to whether there is a simple "risk language" the Board should adopt to focus its dialogue properly and ensure the bases are covered. While each Board must decide for itself whether or not a risk language is useful given the nature of the enterprise's operations, we explore five broad risk categories directors may want to consider as a way of focusing their dialogue with executive management.

We like the five broad risk categories recommended by the National Association of Corporate Directors (NACD). They are: governance risks, critical enterprise risks, Board-approval risks, business management risks and emerging risks. These categories are sufficiently broad to apply to every company, regardless of its industry, organizational strategy and unique risks. More importantly, they provide a context for Boards and management to understand the scope of the Board's risk oversight, as well as the delineation of the Board's oversight responsibilities and management's responsibilities for identifying, evaluating, managing and monitoring risk.

1 Governance risks

These risks relate to directors' decisions regarding Board leadership, composition and structure; director and CEO selection; CEO compensation and succession and other important governance matters critical to the enterprise's success. Often, these decisions require directors to weigh the pros and cons associated with alternative courses of action. While Boards can periodically benchmark their processes for evaluating these matters by considering best practices employed by other Boards weighing similar decisions, they often must rely on their collective business judgment, knowledge of the business and information provided by third-party advisers, including search firms, compensation consultants and legal counsel.

Key point: These matters are exclusively within the Board's domain.

2 Critical enterprise risks

These risks are the ones that really matter, the top five to 10 risks that can threaten the viability of the company's strategy and business model. Certain risks require directors to have the necessary information that will prepare them for substantive discussions with management about how these risks are managed. The criticality of these risks – such as credit risk in a financial institution or supply chain risk in a manufacturer – may require full Board engagement as well as an ongoing oversight process.

While management is responsible for addressing these risks, the Board should consider its own information requirements for understanding management's effectiveness in addressing them. For example, the Board might require management to report on the impact and likelihood of the risk on key strategic goals as compared to other enterprise risks, as well as the status of risk mitigation efforts with input from the executives responsible for managing specific risks. Other examples of relevant information useful to the Board might include the effects of technological obsolescence, changes in the overall assessment of risk over time, the effect of changes in the environment on the core assumptions underlying the company's strategy and interrelationships with other enterprise risks.

Key point: These risks should command a prominent place on the Board's risk oversight agenda. The Board should satisfy itself that management has in place an effective process for identifying the organization's critical enterprise risks so that the Board's risk oversight is properly focused.

3 Board-approval risks

These risks relate to decisions the Board must make with respect to approving important policies, major strategic initiatives, acquisitions or divestitures, major investments, entry into new markets, etc. Through careful consideration and timely due diligence, directors must satisfy themselves that management's recommendations regarding these matters are appropriate to the enterprise before approving them. Therefore, such matters may prompt the Board to ask questions regarding the associated rewards

CONTINUED

and risks and even request further analysis before approving management's recommended actions.

Key point: The matters requiring Board approval are often specified in the corporate bylaws and various charters of the Board and its respective committees. That said, changes in the business may necessitate that the Board and executive management remain on the same page as to what requires Board approval. It is important that the Board approve major strategic and policy issues on a before-the-fact basis.

4 Business management risks

These are the risks associated with normal, ongoing day-to-day business operations. Every business has myriad operational, financial and compliance risks embedded within its day-to-day operations. Because the Board simply does not have sufficient time to consider every risk individually, it should identify specific categories of business risks that pose threats warranting attention and determine whether to oversee each category at the Board level or delegate oversight responsibility to an appropriate committee. For example, the audit committee traditionally oversees financial reporting risks. Other business risks might include: operational risks associated with internal processes, IT, intellectual property, customer service, obsolescence, manufacturing and the environment, financial risks such as excessive leveraging of the balance sheet, compliance risks such as non-compliance with a new complex law and reputational risks such as those that threaten the company's brand image. With respect to all of these risks, it is management's responsibility to address them. If any of them are critical enterprise risks, they warrant the Board's full attention (as noted earlier).

Key point: The Board's committees may oversee many of these risks in accordance with their chartered activities. Typically, periodic reporting coupled with escalation of unusual developments requiring Board attention will suffice.

5 Emerging risks

These are the external risks outside the scope of the first four categories. While management is responsible for addressing these risks, directors may need to understand them. The effects on the business of demographic shifts, climate change, catastrophic events and new cybersecurity threats are examples.

Key point: The Board needs to satisfy itself that management has processes in place to identify and communicate emerging risks on a timely basis. Such processes enable management and the Board to be proactive.

The above risk categories provide a useful context for Boards and executive management to ensure the scope of the risk oversight process is sufficiently comprehensive and focused.

Jim DeLoach
Protiviti

Boardroom Black Holes and Taboos

GARY PATTERSON

Is your Board side-steppng the hard questions? Sure, some subjects are uncomfortable to talk about, but avoiding them isn't a great solution. In some instances, turning a blind eye to a taboo topic could be putting your organization's fiscal health at risk. Is that a gamble you're willing to make? Follow these tips to pinpoint, prioritize and start to address your taboo issues.

When you are cringing in a foxhole dodging shot and shrapnel, it is tough to be strategic, candid and on top of your game. We've all been there from time to time.

Your peers at the National Association of Corporate Directors (NACD) annual Board Leadership Conference Success identified a list of uncomfortable topics that Boards of Directors and CEOs sometimes gloss over. If you are not confronted with some of the problems that these taboo topics reflect, count yourself lucky to be living in the land of milk and honey.

How does this happen?

Pressed by hard financial realities, leaders say they made it through the recession by hunkering down through the mean times and getting lean. They were forced to cut fat, then muscle and finally bone. We all live in a world where there is never enough money, people or time to fix all problems and pursue all opportunities. Leaders can make very bad choices if their organizations do not think through their uncomfortable taboo topics.

Has your organization ever had a fiscal checkup? We're not talking about some bean-counting exercise, but rather an operational and strategic assessment of how your organization reflects the true realities of the world you are living in.

Below are some key areas to help you look for your 800-pound gorilla and to position your Board to better prioritize which issues to address in more detail and in what order.

Over-reliance on information from management.

It is easy to become too insular and rely upon reports and updates from management. Experts are calling for directors to work closer with management in assessing your business and updating strategy. Where might external activists better understand your business than you do?

CONTINUED

The urgent overwhelms the important

Get serious about risk factors and how to mitigate them. This is particularly important for middle market companies that can't afford to make mistakes. Where can you make the enterprise risk management process more strategic and operational in order to build shareholder value?

HR brings sexy back

Many Boards seem to look only at top executives. Everyone talks about people being their most important asset. Where can you improve your human capital base for the top three levels of your people?

Disrupt or be disrupted

Many times disruption comes from outside your industry. People become too complacent, insular or resistant to change. Is your organization a Motorola or Sears, or is it a Google?

Compensation risk profile

Management focus and performance follows reward. Where should incentive plans be tweaked or even rebuilt from the ground up to encourage actions that reflect your best long-term corporate interests versus this quarter's or year's results?

Need to update risk appetite

There always will be tension between the Board and management on how much risk to take on for the reward targeted. How well defined and mutually agreed upon is the risk appetite structure? This includes defined levels of risk that provide parameters for management behavior.

Lack of the right timely information needed for management and leadership

Some organizations' information is forward-looking; other organizations are historically oriented. Management is only as strong as its metrics. Does your organization have the right information to make the right decisions at the right time? How well do you understand and measure the key levers for future growth?

Gold watch syndrome

Have one or more directors retired in place and need to be given a gold watch and a retirement party?

Opportunity costs

Do you keep doing the same things you have always done because it's comfortable? Where should you reallocate resources and think bigger?

Unwilling to take enough risk

Failing fast and cheap in order to learn how to improve beats a long, slow death by inertia. How regularly do you make meaningful bets in terms of money, time and resources for "game changing" initiatives?

The Kodak syndrome

This former great innovator and disruptor now seems to be the poster child for spending too much time doing the wrong things right, but not doing the right things. Where would you benefit from actually going ahead and doing something?

Squandering director skills

What would you do differently if you thought you would lose your three most strategic and operationally focused directors in the next six months?

Political correctness runs amok

More calls for candor are being heard. How often does your Board of Directors err on the side of politeness when actually speaking out is more appropriate?

Updating the business model regularly

What percentage of your activities comes from initiatives that started in the last three years?

Accelerated blurring between nonprofit and for-profit

True North is no longer to maximize long-term profitability. The phrase "economic patriot" is a politically correct way to say "paying too much in taxes compared to most of your foreign competitors." How well prepared is your business to move toward more socially responsible and nonprofit endeavors in the next five years (and preferably 10 years)?

Right person in the right seat driving the bus

Board leadership requires understanding and knowing who the best qualified people are to lead a discussion on a topic or ensure that their voices are heard. Where could you benefit from more contributions from quieter and more appropriate voices on a given topic?

Functional obsolescence

Believe it or not, Windows 98 still exists and people are forced to use it rather than being allowed to upgrade. Where are your opportunities to invest in training and intellectual property to give your people the tools and support needed to increase their contributions to the business?

Back to the basics

Even experienced directors need refreshers and updates. Continuing education is not a luxury, it is a requirement. Why is there such resistance to on-boarding, updates and training? If it was not just your company, but also your personal wealth that was at risk for decisions voted on, where would you encourage refreshers and updates?

Ostrich syndrome or directors in the land of denial

How many of your directors want to believe things are great, rather than truthfully benchmarking your company against other firms in your space or even outside your space?

Pay distribution

The distribution of pay equity from CEO to entry-level workers issue will not go away. How will you move forward on this issue?

Conclusion

Recall the time one of your parents said "speak to your father or mother about that." You knew that meant they did not want to talk about an issue. There is a value in an outsider calling out the ugly baby rather than yourself. What C-level executive or Board member should consider the points outlined above to help them come to grips with seemingly invisible, unforeseeable issues?

Perhaps now is the time to get your organization's house in order: to know, prioritize and fix those high-impact issues that will not go away. With that process, you will better understand your risk profile and be more comfortable that the right big bets are being made on your business. Then, you can worry less about your million-dollar blind spot finding you before you find it.

Gary Patterson
FiscalDoctor

Four Ways Boards Can Strengthen Cybersecurity

RAJ CHAUDHARY WITH CONTRIBUTING AUTHOR **MIKE DEL GIUDICE**

Although well aware of the threat posed by hackers and organized cybercriminals, an alarming number of Boards are not actively challenging management's cybersecurity efforts. Often, Board members simply don't know how to proceed. However, there are concrete actions that directors can take immediately to carry out their governance duties and improve cybersecurity.

With new cyberthreats constantly emerging, directors need to play an active part

Boards of Directors realize the importance of instituting and enforcing cybersecurity measures and enhancing them over time – all in the interest of maintaining the confidentiality, integrity and availability of the organization's assets. It's doubtful, however, that most Boards are administering proper oversight of their organization's cybersecurity training, frameworks and response plans.

What's at Risk

The stakes could not be higher. Data breaches cost billions, damage brands and reduce competitiveness. A large percentage go undetected – and when they are detected, it's an average of 206 days after the incident occurred, according to a study by the Ponemon Institute. And a data breach costs approximately $154 for each record lost.

Cyber crime victims in the past few years have included prominent corporations. For example, Target's data breach in late 2013 potentially compromised approximately 40 million credit and debit cards, and Target reimbursed financial institutions tens of millions of dollars earlier this year.

Security breaches have resulted in shareholder litigation, some of it aimed squarely at Boards. In fact, investors have brought derivative action against Target's Board, claiming that the Board and top executives had failed to take adequate steps to prevent the breach and did not fully disclose to consumers the extent of the theft.

Even though their awareness is high, however, most Boards don't take an active role in cybersecurity. According to a 2015 survey by New York Stock Exchange Governance Services and Veracode, 10 percent of Boards talk about cybersecurity matters "only after [an] internal or industry incident," and 8 percent "only after [a] recent string of high-profile breaches in [the] industry." Alarmingly, the survey also revealed that just one-third of Board respondents are "confident" or "very confident" in their company's cybersecurity.

Board members may wonder what they should be doing to improve cybersecurity. A 2014 survey of directors by the Institute of Internal Auditors Research Foundation and ISACA found that 58 percent believed that they should be "actively involved" in cybersecurity preparedness, but only 14 percent said that they were actively involved and 36 percent reported being "minimally involved."[5]

But what does "active" involvement really mean, and how can directors achieve it?

What the Board Can Do

For the Board, cybersecurity responsibilities are governance-focused, as these tasks are part of Directors' fiduciary duties:

- Provide guidance about their expectations.
- Communicate the right tone and message to management.
- Confirm that the company has implemented security processes and has good cyber incident response plans.
- Work with other Directors and outside entities to gather ideas for overseeing cybersecurity initiatives.

In practice, this means a Board is to provide oversight so that the organization takes adequate cybersecurity measures to cope with existing and emerging threats and, in case of an attack, enacts strong response plans. However, reaching that level of oversight requires Boards to go beyond their usual role of asking management questions.

The following are four ways that Boards can play an important role in strengthening the organization's cybersecurity.

Obtain Cybersecurity Training

Board members don't have to be experts in cybersecurity, but they need to understand the risks to the enterprise and be aware of major trends affecting cybersecurity.

This level of understanding often requires formal training. Training may be as straightforward as requesting information from associations (the National Association of Corporate Directors, for instance), but training usually involves a presentation to the Board by an outside party.

Whatever the training medium, it is critical that directors gain a basic understanding of the complexities of cybersecurity. Cybersecurity is not simply a firewall, virus protection or security patches, but rather a companywide effort involving all employees. It includes the assessment of current threats, the implementation of adequate protection and response plans and the ability to evolve as new (and currently unknown) risks emerge.

Directors should keep up to date with cybersecurity-related developments, both worldwide and in their industries, and the risks and potential legal ramifications the trends present. For instance, hackers today are often organized gangs abroad and might have unofficial government backing. These gangs

CONTINUED

may be interested in more than stealing credit card numbers or customer data; some cybercriminal groups take data hostage, denying companies access and demanding ransom for the data's return. Some hackers (and sometimes rogue governments) may want to create havoc rather than extract money.

Cyber attackers represent systematic, methodical and persistent threats that can change tactics on a dime. Approximately 317 million pieces of malware were created in 2014, and, with a few command changes, hackers can use a piece of malware to create an entirely new threat. Hackers are constantly scanning networks in search of vulnerabilities – and eventually can find holes in almost any network.

Given this challenge, organizations generally have shifted from a breach-avoidance mindset to an acceptance that an incident will occur eventually. Training should provide Boards with an understanding of IT risk management principles so that the directors are better prepared to provide management with feedback on risk tolerance, with the result that all parties have the same understanding of the organization's IT risk posture at any given time.

Conduct a Cybersecurity Maturity Assessment

Having an independent assessment of the company's cybersecurity done is an essential element of a Board's oversight duties. This assessment goes beyond an audit: Organizations need a cybersecurity maturity assessment.

Audits assess control effectiveness at a single point in time. A maturity assessment helps ascertain how well an enterprise can cope with risks that constantly change, and it evaluates the effectiveness and responsiveness of the cybersecurity controls that are in place.

A company's level of cybersecurity maturity can range from nonexistent to optimal. Although dysfunctional or nonexistent cybersecurity operations are unacceptable for any company, not every organization wishes to spend the time and resources required to reach the highest level of maturity. Instead, each company must figure out how much risk it is willing to tolerate and its appropriate maturity level.

The maturity assessment helps Boards push management to figure out where on the risk spectrum the organization wants to reside.

The maturity assessment also helps Boards provide direction and input to help management define a roadmap that guides the company toward greater maturity.

Oversee the Cybersecurity Program

Oversight starts with the Board's determination of whether the company has a framework in place for building adequate cybersecurity defenses and responses. A cybersecurity framework can provide an organization with a starting point. The National Institutes of Standards and Technology cybersecurity framework is a voluntary tool that can assist the Board by providing guidance on controls to consider for the organization's cybersecurity program.

The framework can help directors judge how their companies evaluate risk, provide guidance on controls to consider to manage risk and monitor the organization's risks and controls, for example.

One way for Boards to monitor risk is to work with management to define key risk indicators (KRIs) for the IT organization. KRIs allow management to provide simple dashboards that summarize the cybersecurity risk posture for the organization at that time, and they can provide an early warning when risks are not being managed at an acceptable level. Boards can help determine the KRIs that are tracked and the criteria used to measure the status of current risks.

Another component essential to monitoring risks is strong cybersecurity-related employee communication and training. According to estimates, negligence on the part of personnel is involved in more than 80 percent of data breaches. Employees are prime targets of phishing and spoofing attacks and may download viruses and malware, inadvertently exposing sensitive corporate and client data.

Most companies train employees on cybersecurity at least annually. Boards can insist on more frequent, targeted training modules that focus on individual security issues. Single-topic training modules make it easier for employees to understand individual issues, while increased training frequency helps raise awareness.

Support Cyber Incident Preparedness

Boards set the proper tone for the company, showing management and employees that cybersecurity is a corporate priority. As part of their governance duties, Boards need to confirm that risk management is adequate across the entire enterprise – and that the company is measuring the effectiveness of its security framework and defense measures. Most important, directors need to see that the effort is being allotted the necessary staff, budget and attention.

A Board should also be involved in seeing that a comprehensive incident response plan is in place – that is, that the plan doesn't exist only on paper – and confirming that the plan is tested and revised over time.

Directors need to know their roles in a response plan and be prepared to react accordingly to an incident. They also should be prepared for how all involved parties – including customers, third parties, regulators and law enforcement – are likely to react to a breach.

In the aftermath of an attack and the reaction to it, the Board should review how the company responded and see that improvements are made.

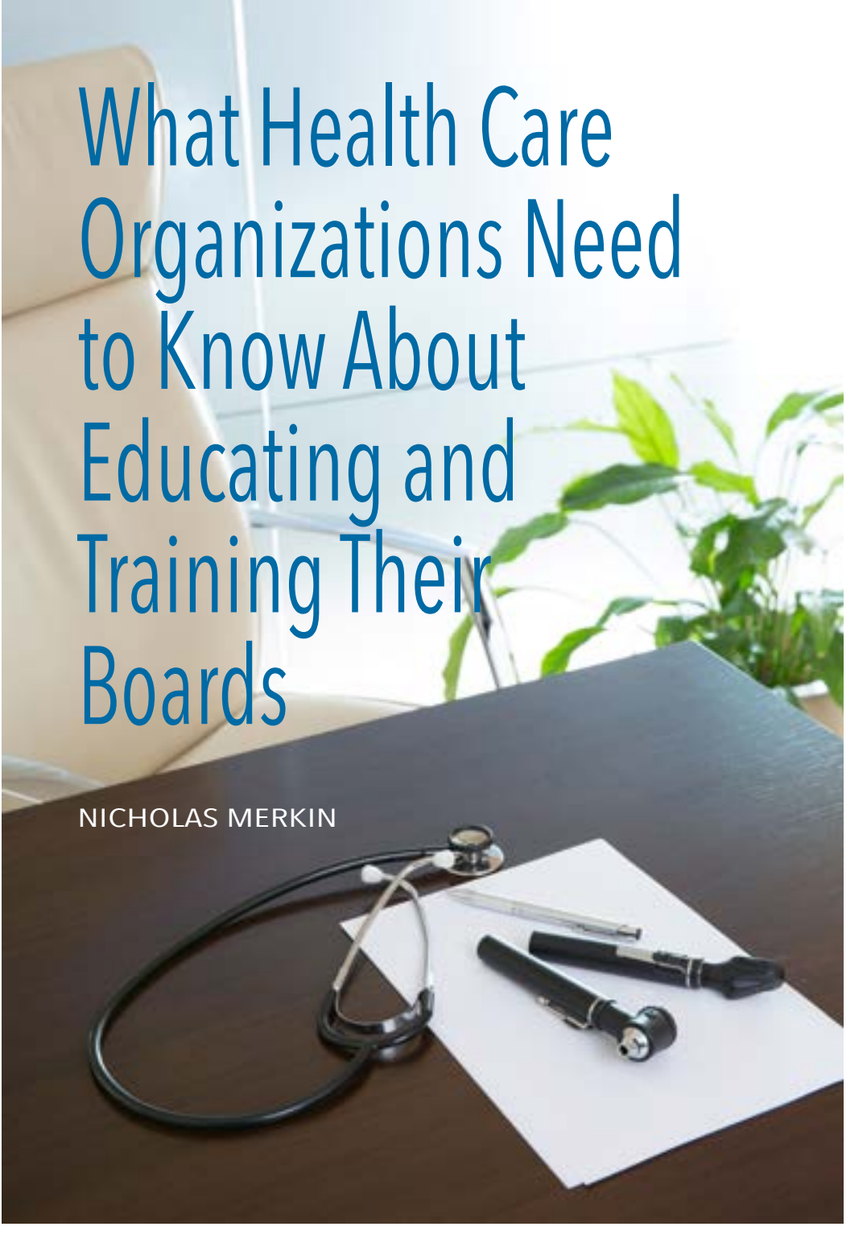
Try to Enjoy the Journey

As is true for many Board responsibilities, cybersecurity is an ongoing journey, not a destination. Directors can envision cyber threats as unethical competitors that release new product offerings every day: More than 99 percent of the products wouldn't affect the company's competitive position, but eventually one could cause an enormous hit to the company's revenue, reputation and even legal standing. There's simply no endgame in cybersecurity.

Raj Chaudhary
Crowe Horwath

What Health Care Organizations Need to Know About Educating and Training Their Boards

NICHOLAS MERKIN



Board members of health care organizations are under more scrutiny than ever as a result of the unique compliance requirements in the health care industry, as well as increased regulatory enforcement and third-party lawsuits.

Board members of health care organizations are under more scrutiny than ever before. As a result of the unique compliance requirements in the healthcare industry, as well as increased regulatory enforcement and third-party lawsuits, health care corporate directors arguably have greater responsibility – as well as liability – than many of their peers in non-health care sectors for the oversight of their organizations' corporate compliance programs.

In this environment, it is crucial for health care entities – typically through an organization's Chief Compliance Officer – to educate and train effectively members of the Board of Directors with respect to their fiduciary duties, as well as the structure and operations of the entity's compliance program. This process should commence well before the CCO's first formal board presentation or the CCO's preparation of compliance oversight metrics. Rather, an in-depth training program for corporate directors should be an ongoing process for new and veteran corporate directors alike and should be fully integrated with the overall obligations of the corporate Board.

The following is an outline for a model educational program for directors that may be implemented by health care organization CCO's and compliance personnel.

Fiduciary Duties and Relevant Regulations

At the most basic level, director training should inform and educate directors as to their various fiduciary duties in connection with the compliance function, as well as the primary regulations that relate to organizational compliance. While a full summary with respect to the fiduciary obligations of corporate directors and relevant health care regulations is well beyond the scope of this article, at a minimum, directors should be advised as to their duties of care and good faith dealings, including the duty of reasonable inquiry, the Caremark decision standards and the business judgment rule. Additionally, directors should have an awareness of relevant regulations, such as the False Claims Act, Stark and Anti-Kickback laws, exclusion screening requirements, HIPAA and other privacy laws, as well as applicable state laws.

Policies and Procedures and Code of Conduct

Written policies and procedures are a roadmap for health care organizations that help them mitigate day-to-day compliance risks. The policies and procedures should address all details of the compliance function from reimbursement to quality issues. Like all guidebooks, an organization's policies and procedures should be in a constant process of revision in response to changing laws and regulations, as well as compliance concerns. Members of the Board should be familiar with both the substance of their organization's policies and procedures and the mechanism by which the policies and procedures are revised and kept current.

Additionally, an organizational code of conduct articulates to staff, patients and management the healthcare entity's commitment to the ethics and values underlying corporate compliance. Similar to an organization's policies and procedures, the code of conduct should be periodically updated for relevance and applicability. Moreover, all decisions of management and the corporate Board should be consistent with the organization's code of conduct. The code of conduct, as well as its process of revision, therefore, should be meaningfully communicated to the Board of Directors and throughout the organization.

Written policies and procedures are a roadmap for healthcare organizations that help then mitigate day-to-day compliance risks.

The Structure of the Corporate Compliance Program

Directors should be made aware of the structure of their organization's compliance program. All directors should be familiar with the key employees responsible for the program's operation, the functioning of the program, how the Board is to receive information and monitor their organization's compliance program and compliance issues that may arise and what metrics are available to assess the efficacy of the current compliance infrastructure. Board members should know what, when and how relevant compliance-related information will be received and understand what tools they will have to assist in the Board's decision making.

Importantly, Board members should have access to benchmarks and other information regarding how the health care organization has handled compliance issues in the past, how current performance compares to prior performance, current and past enforcement actions and lawsuits and the procedures for self-reporting when wrongful conduct is uncovered.

Members of the Board should also be knowledgeable as to their organization's risk profile, how it was determined, and what resources – both financial and human – are available to the organization to address compliance needs.

Last, directors should understand what their organization – and specifically the CCO – is doing in connection with prospective compliance planning. Compliance is never a static function and organizations' future compliance programming should be responsive to both governmental enforcement

CONTINUED

priorities and entities' fluid risk profiles.

The Function of the Compliance Program

The overall function of an organization's compliance program is perhaps the most challenging aspect of Board education and training. It is unrealistic to assume that directors will become expert in all areas and in all details of compliance infrastructure. That said, it is important that members of the Board be sufficiently familiar with the following areas of the operation of their organization's compliance programming:

- Delegation of authority and areas of accountability with respect to the compliance program and its implementation, as well as the separation of powers and responsibilities among the CCO, General Counsel, human resources, senior management, the Board of Directors and any compliance subcommittees of the Board or management.
- The level and mechanism for compliance training across the organization and the enforcement of entity training and knowledge standards, including the documentation of such training and audits of personnel knowledge.
- The mechanisms and systems in place for compliance program flexibility in light of regulatory or industry change.
- The day-to-day operations and details of areas within the organization where significant compliance risk has been identified and the timeline for remediation of those risks.
- The mechanisms in place for detection of possible compliance violations, including the compliance hotline, internal compliance surveys, compliance incident reports and staff self-reporting. Most crucially, directors should be aware of possible violations pending resolution and related timelines and the going forward planning designed to avoid future violations.
- Whistleblower and employee protection controls and the appropriate use of inside and outside legal counsel, as well as the functioning of attorney-client confidentiality and attorney work product protections.
- The operation of the organization's quality improvement program, including relevant entity metrics and areas of accountability for key personnel.

Conclusion

As demonstrated above, effective education of health care entity Boards is a formidable challenge, but an important one. An effective corporate director training program requires a significant investment in time and resources, but is crucial to overall compliance oversight and organizational health. Although there is no such thing as a "one-size-fits-all" Board training program, the foregoing is a useful topical model for use by CCOs and their staffs. There are also many written products available on the market addressing issues of director responsibilities and education, as well as independent consulting firms providing useful programming in this area. At bottom, a robust training program for corporate directors of healthcare organizations will empower directors to discharge their oversight obligations regarding corporate compliance and minimize overall legal and governmental enforcement risk.

Nicholas Merkin
Compliagent

Five Ways to Ensure Board Support for Compliance

MICHAEL VOLKOV

It's absolutely critical that the Chief Compliance Officer and the Board of Directors work together to achieve a culture of ethics and compliance. With the Board's backing, a CCO's influence is far greater. Establishing that relationship, however, may be a daunting proposition.

A Chief Compliance Officer has a number of important relationships to maintain in an organization. Aside from the support of senior-level executives, the CCO has to build an effective working relationship with the Board and the relevant Board committee responsible for ethics and compliance.

From an operational standpoint, a CCO has to use the Board to advance an issue when frustrated by senior management. A CCO's direct contact with the Board gives the CCO an important tool that should be used in rare situations to ensure that senior management properly attends to the ethics and compliance function.

To accomplish this important bond, a CCO has to undertake five important steps:

1 Create a Personal Relationship

A CCO has to devote time and attention to establishing personal relationships with the chair of the committee (assuming it is an audit committee) responsible for oversight of the company's ethics and compliance program. I hate to sound like a "relationship advisor," but a CCO has to schedule regular meetings, telephone calls and/or meals with the chair of the audit committee to discuss issues. The CCO has to take the initiative to contact the chair and establish a regular informal communications avenue.

2 Request Sufficient Time to Report to the Board Committee and an Executive Session

A CCO needs, at a minimum, 30 minutes, and preferably 45 to 60 minutes, at every Board committee meeting to present a report of the status of ethics and compliance issues. The meeting has to be face-to-face and should be based on a written report to accompany the oral presentation. An executive session should be included at the conclusion of the presentation so that everyone has an opportunity to discuss issues. A CCO should not use such a session to complain or gossip – instead, this is a valuable opportunity to have a frank discussion about progress and roadblocks to a company's ethics and compliance program.

3 Report on Real and Tangible Ethics and Compliance Issues

A CCO who presents fancy bar graphs and pie charts to establish how many people have been trained, the number of complaints, how many certifications have been collected and the number of internal investigations is wasting the opportunity to gain the audit committee's support, buy-in and initiative. A CCO's compliance report should be tailored to three important issues: (1) the company's culture and how effectively it is being embraced, (2) the company's risk profile and how those risks are being mitigated and managed and (3) identification of significant threats to the company from an ongoing internal or government investigation.

4 Educate the Board on Ethics and Compliance Issues

A CCO's report is an important opportunity to "educate" the Board in ethics and compliance issues. Board members are always interested in new ideas, and ethics and compliance issues should be presented in a way to promote discussion of new approaches and best practices. As part of this effort, it is important to bring up benchmarking, best practices and developments in the ethics and compliance field.

5 Seek the Board's Input on Ethics and Compliance Issues

A CCO should not be a talking head at a Board meeting. It is important for the CCO to engage the Board, enlist the participation of Board members in a discussion and seek their guidance and input on important compliance issues. In this respect, a CCO should study and know each Board member's background, business experience and knowledge with respect to compliance issues. It is important to understand the strengths of each Board member and to encourage their participation on key issues. A Board member will often have prior experiences relating to ethics and

"A chief compliance officer shouldn't be a talking head at a Board meeting..."

compliance issues and their perspective and contribution should be reinforced during any discussion. A CCO has to exercise great care in seeking such input, tailoring it to the ethics and compliance objectives and building a key alliance with the Board on important issues.

Michael Volkov
Volkov Law

Boards of Directors and Compliance: Four Areas of Inquiry

TOM FOX

Compliance programs are made up of lots of moving parts. This four-part approach lays out a clear and logical program for a Board of Directors not only to understand its role in the compliance function, but to play it effectively.

In an article in the December 2011 issue of Compliance Week magazine entitled "Board Checklist: What Every Director Should Know," author Jaclyn Jaeger reported on a panel discussion at the Association of Corporate Counsel's 2011 Annual Meeting, held in October. The discussion was centered on four core areas upon which directors should focus their attention: (1) structure, (2) culture, (3) areas of risk and (4) forecasts. The article focuses on each of these areas, as well as some questions panel participant Amy Hutchens -- General Counsel and Vice President of Compliance and Ethics at Watermark Risk Management International -- suggested a board should ask of the company's Chief Compliance Officer (CCO) or General Counsel.

Structure Questions

This area consists of questions that will aid in determining the fundamental sense of a company's overall compliance program. The questions should cover the basics of the program through to how the program operates in action. Hutchens believes that such inquiries should allow each Board member to communicate the main elements of a compliance program. With those concepts in mind, Hutchens suggests that Board members ask some of the following:

- Who oversees the operation of the program?
- What is in the code of conduct? Is each Board member aware of corporate standards and procedures?
- How are complaints received?
- Who conducts investigations and acts on the results?
- What corporate resources are being devoted to the compliance and ethics program?
- How much money is allocated to the program?
- What type of training is required? How effective is it?
- Have any compliance failures been detected? If so, how were the failures detected?
- If a company's compliance program is less mature, what are the charter compliance documents?
- If a company's compliance program is more mature, there should be queries regarding the roles of the General Counsel vs. a Chief Compliance Officer. If a CCO is required, where would such person sit in the organization and what is the CCO reporting structure?

Culture Questions

This area of inquiry should focus on the culture of the organization regarding corporate compliance. Board members should have an understanding of what message is being communicated not only from senior management, but also middle management. Equally important, the Board needs to understand what message is being heard at the lowest levels within the company. Hutchens suggests that Board members ask some of the following:

- When did the company last conduct a survey to measure the corporate culture of compliance?
- Is it time for the company to resurvey to measure the corporate culture of compliance?
- If a survey is performed, what are the results? Have any deficiencies been demonstrated? If so, what is the action plan going forward to remedy such deficiencies?
- Did any compliance investigations arise from a cultural problem?
- Regardless of any survey results, what can be done to improve the culture of compliance within the company?
- If there were any acquisitions, were they analyzed from a compliance culture perspective?
- If there are any M&A deals on the horizon, have they been reviewed from the compliance perspective?

Areas of Risk Questions

Here Hutchens recommends that Board members know what process is being used to identify emerging risks." Such risk analysis would be broader than simply a legal/compliance risk assessment and should be tied to other matters such as "business continuity planning and crisis response plans." Another panel participant, Jennifer MacDougall, Senior Counsel and Assistance Secretary of Jack-in-the-Box, noted that "the Board of Directors need to use their expertise and ask the right questions:

- What is the risk assessment process?
- How effective is this risk assessment process? Is it stale?
- Who is involved in the risk assessment process?
- Does the risk assessment process take into account any new legal or compliance best practices developments?
- Are there any new operations that pose substantial compliance risks for the company?
- Is the company tracking enforcement trends? Are any competitors facing enforcement actions?
- Has the company moved into any new markets which impose new or additional compliance risks?
- Has the company developed any new product or service lines which change the company's risk profile?

Forecast Questions

Hutchens believes that "a truly effective and informed Board knows where the company stands not only at the present moment, but also has the strategic plan for how the compliance and ethics program can continue to grow." My colleague Stephen Martin suggests that such knowledge is encapsulated in a 1-3-5-year compliance game plan.

However, a compliance program should be nimble enough to respond to new information or actions such as mergers or acquisitions, divestitures or other external events. If a dynamic changes, "you want to get your Board's attention on the changes which may need to happen with the [compliance] program." Hutchens believes that such agility is best accomplished by obtaining buy-in from the Board through it understanding the role of forecasting the compliance program going forward.

The four-part approach suggested by Hutchens lays out a clear and logical program for a Board of Directors not just understand its role in the compliance function but to play an active role. Any best practices compliance program has several moving parts: a CCO to lead the compliance program, a compliance department to execute the strategy and an engaged Board of Directors who oversee and participate. We applaud Hutchens' approach and commend it for use by a company's Board of Directors.

Tom Fox
Tom Fox Law

AUTHORS

Michael Volkov *is the CEO of The Volkov Law Group LLC, where he provides compliance, internal investigation and white collar defense services. His practice focuses on white collar defense, corporate compliance, internal investigations and regulatory enforcement matters. He is a former federal prosecutor with almost 30 years of experience in a variety of government positions and private practice. He has extensive experience representing clients on matters involving the Foreign Corrupt Practices Act, the UK Bribery Act, money laundering, Office of Foreign Asset Control (OFAC), export controls, sanctions and International Traffic in Arms, False Claims Act, Congressional investigations, online gambling and regulatory enforcement issues. directors and professionals in, internal investigations and criminal and civil trials.*

Stuart Altman *is a partner at Hogan Lovells US LLP. His practice includes white collar criminal investigations and defense, including representation of clients, conducting internal investigations, compliance and corporate governance matters and complex civil litigation. He has extensive experience representing businesses and individuals in criminal investigations and prosecutions, both as targets and witnesses. He has conducted numerous internal investigations for companies facing criminal and civil liability and has advised clients on how to minimize risk. He has represented a variety of public companies, financial institutions and individuals in investigations and proceedings before the SEC, other agencies and self-regulating organizations.*

Gary W. Patterson, *President & CEO of FiscalDoctor®, works with leaders who want to uncover their blind spot, before it finds them, so that they can make better decisions. He is a well-known speaker on enterprise risk management (ERM), operational risk management (ORM), strategic budgeting, risk assessments, leadership and change management. Patterson is the author of the 2015 book, Million Dollar Blind Spot.*

Dr. Linda Henman *is one of those rare experts who can say she's a coach, consultant, speaker and author. For more than 30 years, she has worked with Fortune 500 companies and small businesses that want to think strategically, grow dramatically, promote intelligently and compete successfully today and tomorrow. Some of her clients include Emerson Electric, Boeing, Avon and Tyson Foods. She was one of eight experts who worked directly with John Tyson after his company's acquisition of International Beef Products, one of the most successful acquisitions of the twentieth century.*

Daniel J. Hurson *has been a trial lawyer and litigator for more than three decades, with substantial experience in white-collar criminal and securities fraud cases. He has tried cases for the government both as an Assistant U.S. Attorney in Maryland and later in his career as Assistant Chief Litigation Counsel for the Enforcement Division of the SEC in Washington. He represents individuals and corporations before the Enforcement Division of the Securities and Exchange Commission (including insider trading and accounting fraud cases), before the Financial Industry Regulatory Authority, and in matters brought by the DOJ and other federal agencies.*

Thomas Fox *has practiced law in Houston for 25 years and is now assisting companies with FCPA compliance, risk management and international transactions. He was most recently the General Counsel at Drilling Controls, Inc., a worldwide oilfield manufacturing and service company. He was previously Division Counsel with Halliburton Energy Services, Inc. where he supported Halliburton's software division and its downhole division. He writes and speaks nationally and internationally on topics ranging from FCPA compliance, indemnities and other forms of risk management, to tax issues faced by multinational U.S. companies, insurance coverage issues and protection of trade secrets.*

Raj Chaudhary, *CGEIT, CRISC, has more than 30 years of experience in the field of information systems. He is a principal in the Risk Consulting business unit of Crowe Horwath LLP and SVP of Risk Consulting at CHAN Healthcare. He has been the global lead for cybersecurity solutions for Crowe since 2006. He has published numerous articles on the topic of cybersecurity and has presented on this topic to Boards of Directors and management of entities across multiple industries.*

Nicholas Merkin *is Chief Executive Officer of Compliagent, a regulatory consulting firm that designs, manages and maintains compliance programs for health care providers. His clients benefit from his deep understanding of changing state and federal laws and policies as they relate to organizational governance issues, compliance auditing and training, the Stark Law, the Anti-kickback Statute, HIPAA privacy and security and the False Claims Act.*

Launched in December of 2008 and sponsored by Conseli-um, Corporate Compliance Insights is a knowledge-sharing forum designed to educate and encourage informed interaction within the corporate compliance, governance and risk community.

Corporate Compliance Insights combines featured articles written by some of the most experienced compliance and ethics professionals in the world with regular updates of important news events in the world of governance, risk, and compliance. Additionally CCI offers an events calendar, training & resource library and compliance jobs board.

CORPORATE COMPLIANCE INSIGHTS