BOARD OVERSIGHT OF CORPORATE CULTURE 1:15 PM

Jim Duffy, NYSE

Greg Holland, MPS Group, Inc.

Michael Kirwan, Foley & Lardner LLP

Alice Peterson, Syrus Global

Mary Sawall, Huron Consulting

JAMES DUFFY

EXECUTIVE VICE-PRESIDENT &
GENERAL COUNSEL
NYSE

James F. Duffy is an Executive Vice President and the General Counsel of NYSE Regulation, Inc. Since joining the New York Stock Exchange in 1999, Jim has been extensively involved in both domestic and international listings matters, market regulation and market structure issues. Jim was centrally involved in the formulation of the Exchange's expanded corporate governance listing standards, and in the changes to the Exchange's own governance structure as well.

Previously, Jim served for ten years as General Counsel of the American Stock Exchange. Earlier he practiced corporate and securities law on the legal staff of GTE Corporation, and with the firm of Lord, Day & Lord in New York.

MICHAEL B. KIRWAN
OF COUNSEL
FOLEY & LARDNER LLP

Michael B. Kirwan is of counsel in Foley's Transactional & Securities and Private Equity & Venture Capital Practices. He counsels business clients in corporate organization, finance and securities. Mr. Kirwan has worked on numerous public and private offerings, represented many companies on their periodic reporting obligations and handled a variety of business combinations and venture capital matters.

Prior to joining Foley, Mr. Kirwan was a partner in the Corporate Finance Department at LeBoeuf, Lamb, Greene & MacRae, L.L.P. He then became the executive vice president and chief operating officer for a technology consulting firm, Encore Development of North America, Inc.

Mr. Kirwan received his J.D. from Harvard Law School in 1988. He received his bachelor's degree, *magna cum laude*, from Duke University in 1984.

Mr. Kirwan is admitted to practice in Florida. He is a member of the Jacksonville Chamber IT Council, The Florida Bar, and the Jacksonville Bar Association.

Mr. Kirwan has served on numerous civic and charitable boards and is a past chairman of the City of Jacksonville's Ethics Commission. He has written several articles for various Florida Bar publications. Mr. Kirwan was recognized by the *Jacksonville Business Journal* in its 2002 List of Northeast Florida's "Up and Comers."

ALICE PETERSON
PRESIDENT
SYRUS GLOBAL

Alice Peterson is the President of Syrus Global, a leading provider of ethics and compliance solutions headquartered in Chicago. Ms. Peterson founded the company in 2002. She previously held executive positions at PepsiCo, Kraft and Sears. Ms. Peterson serves on the board of directors of Hanesbrands.

Syrus Global's mission is to help enterprises develop and sustain a culture of ethically achieving economic success. Using the company's Listen Up™ ethics reporting/helpline solution, employees at all levels in any type of organization are able to confidentially report wrongdoing and receive help in dealing with ethical dilemmas. The Listen Up approach ensures the highest levels of governance and efficiency. Through customized and engaging content, the company's Rules + Values™ online ethics education delivers relevant and effective learning to employee groups. Syrus Global's Anonymous Interviews allow clients to glean important information from exiting employees and other groups.

From 1989 through 2000, Ms. Peterson held senior positions at Sears, Roebuck and Co. She ran Sears Online from 1998 through 2000, overseeing significant growth in web-related revenues. She was the Vice President and Treasurer of Sears from 1993 through 1998, during which time she spearheaded many of the company's major transformation efforts, including the IPO's and spin-offs of Allstate and Dean Witter Discover.

Ms. Peterson also serves on the boards of Williams Partners, RIM Finance (a wholly owned unit of Research in Motion, maker of the BlackBerry™ handheld). She is a member of the board of directors of the Institute for Business & Professional Ethics at DePaul University and the National Association of Corporate Directors Chicago Chapter.

Ms. Peterson holds an M.B.A. from Vanderbilt University's Owen Graduate School of Management, and a B.A. from the University of Louisville.

MARY SAWALL
VICE-PRESIDENT, HUMAN RESOURCES
HURON CONSULTING GROUP, INC.

Mary M. Sawall is Huron Consulting Group's Vice President of Human Resources and one of the founders of the Company.

Huron is a leading provider of financial and operational consulting services. The Company was founded in May 2002 and has grown from approximately 200 people to more than 1000 today. In October 2004, Huron became a public company listed on the NASDAQ Global Select Market under the symbol HURN.

Huron was named the No. 1 fastest growing new business by *Entrepreneur* magazine in 2005, and again in 2006. In addition, *Consulting Magazine* named Huron one of the ten best consulting firms to work for in 2006. Ms. Sawall and her Human Resources team have been an integral part of Huron's growth and success in the marketplace.

Previously, Ms. Sawall was an Executive Vice President of Human Resources at Encore Development, a technology solutions provider, and at Whittman-Hart Inc., a global business and technology solutions provider. She has also served as Director of Human Resources for the Illinois practice of Deloitte & Touche LLP. In addition, she has held financial and administrative management positions at Booz Allen Hamilton, a global strategy and technology consulting firm and Cambridge Associates, a provider of investment and financial research and consulting services to nonprofit institutions.

Ms. Sawall holds a MBA from Cornell University's Johnson School of Management, a MA from Yale University and a BA from the University of Notre Dame.

Speech by SEC Staff:
Second Annual General Counsel Roundtable:
Tone at the Top: Getting it Right

by

Stephen M. Cutler

Director, Division of Enforcement
U.S. Securities and Exchange Commission

Washington, D.C.
December 3, 2004

An awful lot of people seem to be paying an awful lot of attention to "tone at the top" these days. Articles are being written about it. Speeches (in addition to this one) are being given about it. "Tone at the top" seems to have become a panacea for what is ill in corporate America, and an explanation for much of what has gone wrong.

And I'm sure I don't have to tell you that much has gone wrong. Allow me to spend just a few minutes recapping the last couple of years from an SEC enforcement perspective - and actually, as is the case with all of my remarks today, from my own personal perspective and not the perspective of the Commission or other members of the Commission staff. In the last two fiscal years, the SEC has brought more than 1,300 civil cases and has obtained orders for disgorgement and penalties in excess of $5 billion. These numbers far exceed those of any other two-year time frame in the Commission's history. In this same period, the Department of Justice has brought criminal cases alleging securities-related misconduct by more than 500 defendants.

But it's a recitation of the names (and not the numbers) that I think best conveys a sense of the period that we've been through. In the accounting and financial reporting area, the subjects of our enforcement actions in the last two years include: Enron's Ken Lay, Jeff Skilling, and Andy Fastow and their bankers, Merrill Lynch, Citigroup, J.P. Morgan/Chase and CIBC; WorldCom, Bernie Ebbers and Scott Sullivan; HealthSouth and Richard Scrushy; Qwest; Tyco and Dennis Kozlowski; Hollinger, Conrad Black and David Radler; Adelphia and the Rigases; Lucent Technologies; Parmalat; Gateway Computer; Peregrine Systems; Ernst & Young; General Electric; Schering-Plough and Richard Kogan; Royal Dutch Shell; Halliburton; Gemstar/TV Guide, Henry Yuen and Elsie Leung; Grant Thornton; Computer Associates and Sanjay Kumar; Warnaco and Linda Wachner; Homestore; Symbol Technologies and Tomo Razmilovic; AIG; Wachovia; Vivendi and Jean-Marie Messier; Xerox, Paul Allaire, Richard Thoman, Barry Romeril and KPMG; Royal Ahold; and PriceWaterhouseCoopers.

In the mutual fund area: Pilgrim & Baxter, Harold Baxter and Gary Pilgrim; Alliance Capital; Heartland Advisers; Banc One; Janus; Strong Capital Management and Richard Strong; Conseco; Invesco and Raymond Cunningham; Putnam; Fleet; AIM; MFS; van Wagoner Capital Management and Garrett van Wagoner; Franklin Advisers; and Pimco Equity Advisers and Stephen Treadway.

In the broker-dealer area: Raymond James; Banc of America Securities; UBS PaineWebber; TD Waterhouse; Morgan Stanley; J.P. Morgan Securities; Goldman Sachs; Credit Suisse First Boston; Fidelity Brokerage; Robertson Stephens; Deutsche Bank, Thomas Weisel, Jack Grubman, Henry Blodget and all of the firms involved in the global settlement; SG Cowen and Lehman Brothers; and Spear Leeds, LaBranche, Van der Moolen and all of the other New York Stock Exchange specialist firms.

It takes your breath away. But what does this have to do with tone at the top? One of the connections is probably obvious to everyone here: that is, in so many of the cases I've just cited, the tone at the top couldn't have been all that . . . well, pretty. Indeed, in the last two plus years, we have sued in the neighborhood of 100 public company CEOs. And if CEOs were themselves breaking the law, then they couldn't have been setting a particularly melodious tone.

But there's another, perhaps less obvious connection between what we've been doing in the enforcement arena and tone at the top - and for these purposes, I want to focus on the penalties we have sought and obtained not from the individuals we have charged, but from the institutions with which they were affiliated. Violations of the securities laws are very frequently the product of both individual failings and a deficient corporate culture. Among other things, a complex accounting fraud rarely can be accomplished by one or two rogue employees, acting on their own. It ordinarily takes, as the junior senator from New York might say, a village. And therein lies the answer - or at least an answer - to the question why we've sought penalties not just against individuals, but against companies, too: We're trying to create an environment that reduces the risk of misconduct at all levels of a company - an environment in which the people who run public companies will do more than simply keep themselves out of jail.

In short, we're trying to induce companies to address matters of tone and culture. We're trying to get the fundamentally honest, decent CEO or CFO or General Counsel - the one who wouldn't break the law - to say to herself when she wakes up in the morning: "I'm going to spend part of my day today worrying about, and doing something about, the culture of my company. I'm going to make sure that others at the company don't break the law, and don't even come close to breaking the law."

What we're asking of that CEO, CFO or General Counsel goes beyond what a perp walk or an enforcement action against another company executive might impel her to do. We're hoping that if she sees that a failure of corporate culture can result in a fine that significantly exceeds the proverbial "cost of doing business," and reflects a failure on her watch - and a failure on terms that everyone can understand: the company's bottom line - she may have a little more incentive to pay attention to the environment in which her company's employees do their jobs.

So when we impose penalties on the order of $750 million against WorldCom or $250 million against Qwest or $100 million against Bristol-Myers Squibb or $100 million against Alliance Capital, what we're really targeting are the hearts and minds of senior executives. We want them to know that there are serious, real-world consequences to them if their institutions fail to adhere to the law - even if they aren't themselves scofflaws.

Of course, the flip side of this approach is that we have to reward companies that, notwithstanding a violation of the law, can demonstrate that they had or have made significant efforts to achieve a culture of compliance. So, if you look at the Commission's 21(a) report in the Seaboard matter, you'll see that the Commission seeks to recognize, in its charging and sanctioning decisions (and in its decisions not to charge and not to sanction), efforts by companies to police themselves, report problems to the government and establish a solid culture of compliance.

And by the way, we're not alone in our concern with these matters. The Department of Justice (in the Thompson memo), and the U.S. Sentencing Commission (in the sentencing guidelines) have emphasized the need for companies to have strong ethics and antifraud programs. So has Congress - in the form of statutory requirements that CEOs and CFOs certify financials and put in place effective disclosure and internal controls. That's why I want to address a subject that's ordinarily left to business people, business schools, and business psychologists. No, I've never run a public company; and no, I don't profess to be an expert in the area. But I do have some suggestions gleaned from my own experience as a regulator, prosecutor, and even as a manager of a large group of staff. And all of my suggestions boil down to this: You've got to talk the talk; and you've got to walk the walk. Both are critical to maintaining a good tone at the top. Let me flesh that out a bit.

Talking the Talk

First, talking the talk: From an employee's first day on the job to the day he gets his gold watch, he should know that ethics and honesty are important at your company. And how should he know that? Because you've told him so. Every company - it really should go without saying - must have a strong code of ethics and a set of written policies and procedures to enforce and reinforce those standards.

But it's not enough just to put those documents in the company manual that you hand out at orientation or trot out once a year. You have to talk about the company's ethical standards again and again. Those standards have to infuse the day-to-day lives of your employees. What does that mean? Ethics and compliance should be part of your regular education and training efforts - and I mean efforts that go beyond perfunctory lectures about legal requirements, but embrace well-conceived, real-life situations and dialogue. It also means that whenever your CEO is delivering a state-of-the-company address to company employees, or offering remarks at a company event, she should be talking about the company's values as well as its profits. Too many times in our cases, we've seen instances of senior managers demanding "results," and what employees heard was a demand for "results at any cost - including non-compliance with the rules."

What's more, it has to be senior management - not just the legal department, the compliance professionals, or human resource experts - that does the talking. Matters of ethics and culture shouldn't be shunted off to the outer edges (or cost centers) of a corporate organization. In order to convey the importance of integrity and honesty to a corporation's employees, those who run the business, those who are responsible for the bottom line, have to be the ones to tell employees that integrity and honesty matter. For if they don't do it, employees won't believe that those values are core values; they won't believe that integrity and honesty are important to those who really matter; they won't believe that their path to success will require adherence to those values. So when you take your ethics road show to your employees, have your most senior managers play an active role. I know of a very large financial services firm where the CEO is planning to have a series of dinners with all of the company's high-level supervisors all over the world to discuss compliance issues. The object is to instill in employees the notion that these issues are important - or, as Chairman Donaldson has said, to make ethics part of the company's DNA.

And no double talk. You can't say to the broad audience that ethics, integrity and honesty are important, but ignore them (or worse yet, joke about them or dismiss them) when you're in a social setting, or "off line," or off the record, or when you're talking to smaller groups. At Enron, we know that senior managers conducted a skit in which one of the themes was deceiving the SEC. That probably didn't help create a culture of respect for the law. At Hollinger, Conrad Black wrote an email in which he referred to his company's shareholders as "a bunch of self-righteous hypocrites and ingrates." Finally, what no double talk also means is that if something goes wrong, if there is an ethical or legal lapse, be candid about it, acknowledge it, and don't try to minimize it. Instead, tell your employees (and the world at large) that it shouldn't have happened and that it's inconsistent with the kind of company you want to be.

Let me make just two more points about talking the talk: First, in an ideal world, the talk should extend beyond your company's own walls - to those with whom your company does business - vendors, consultants, customers, contractors, etc. Over the past year, a number of our cases have included charges against such third parties: for sending false invoices or audit confirmations, for engaging in fraudulent round-trip transactions and for otherwise facilitating or aiding a public company's fraudulent schemes. Without their complicity, the public companies with which they had dealings may not have been able to violate the law. Clearly, and this is something that Ben Heineman at G.E. preaches, it's important to deliver the message of integrity, honesty and truthfulness to those with whom you do business.

Second, as this audience is well aware, good communication means speaking and listening in equal parts. To know what ethical issues your employees face, to really get a sense of them, you've got to be able to listen to your employees' concerns. This means ensuring that there is a safe, reliable and well-known avenue of communication open to those who have ethical questions or who want to report possible compliance shortcomings. Empower employees to identify possible misconduct - indeed, consider requiring employees to identify it when they're aware of it. As the head of the Commission's examination program, Lori Richards, has said, "be[] ready and able to hear bad news." And make it clear that retaliating against or threatening a whistle-blower will not be tolerated and will be viewed as a "fire"-able offense.

Sarbanes-Oxley requires that a listed issuer's audit committee establish procedures for the confidential submission of concerns regarding questionable accounting or auditing matters. Let me offer an additional suggestion: the appointment of a permanent ombudsman or business practices officer to receive and investigate complaints - a private inspector general, if you will. That person might report to the audit committee to ensure his independence, and also to ensure that company's board is fully aware of emerging ethical or legal issues reported by company employees.

As part of its settlement with Qwest, the Commission required the company to permanently maintain such a position. And while I don't mean to equate Qwest's situation with that of other companies, I do think the position makes sense, both practically, as a way to catch and resolve problems before they metastasize, and symbolically, as an institutional commitment to the importance of ethics, integrity, and legal compliance.

Walking the Walk

That brings me to walking the walk. All the words in the world mean nothing without deeds to support them. You have to pay more than lip service to values. You have to live them. The last few years have provided any number of examples of companies that failed to practice what they appeared to preach. Enron had the corporate slogan of "Respect, Integrity, Community, Excellence." To the employees and shareholders who lost their pensions or their life savings in the fraud, the words of that slogan ring rather hollow. In October 2003, at a conference of corporate directors, then Chairman and CEO of Computer Associates Sanjay Kumar bragged about his company's state-of-the-art corporate governance and business ethics practices. At the same time, according to the cases filed against him, Mr. Kumar was engaged in a large-scale fraud. As former IBM CEO Lou Gerstner has said, "you can't simply give a couple of speeches or write a new credo for the company and declare that a new culture has taken hold. You can't mandate it, can't engineer it. What you can do is create the conditions for transformation. You can provide incentives."

So here is my own, underinclusive, idiosyncratic list of ways in which a company can do just that:

First, and I guess this is rather obvious: managers themselves have to comply with the letter and the spirit of the rules. Employees watch what their managers do as well as say - they scrutinize their every move and follow their lead. If employees see managers bend the rules, they'll bend the rules.

That applies to the smallest of rules. If all employees are required to attend the company's ethics training program, then senior management should be attending the training too. They can't just say, "well, that's for the others, I don't need to do that."

Second, make character a part of the firm's set of key hiring criteria. Or, to borrow a phrase from Jim Carville: "It's the people, stupid." If you can attract and retain people of good moral character, you've won half the battle. As one company executive recently put it to me, "It's the reverse of the 'meatball magnetism' theory. Meatballs might be attracted to one another, but so are honest people. Hire a bunch and you're likely to get more." Think about this in a serious way when you hire entry-level employees - go beyond the background check designed to determine whether the prospective employee has a criminal record or was kicked out of school or fired from the last job.

Third, and this really follows from the last point: make integrity, ethics and compliance part of the promotion, compensation and evaluation processes as well. For at the end of the day, the most effective way to communicate that "doing the right thing" is a priority, is to reward it. Conversely, if employees are led to believe that, when it comes to compensation and career advancement, all that counts is short-term profitability, and that cutting ethical corners is an acceptable way of getting there, they'll perform to that measure. To cite an example from a different walk of life: a college football coach can be told that the graduation rates of his players are what matters, but he'll know differently if the sole focus of his contract extension talks or the decision to fire him is his win-loss record.

Fourth, make it clear that you won't tolerate compliance risks - even if that means losing a lucrative piece of business or a client or a transaction. Convey, with your actions, that your company's long-term reputation and success are more important than short-term profitability. When he was the general counsel of PaineWebber, Ted Levine said, "good compliance is good business." After all, as we have too frequently seen, the financial costs of non-compliance can be terribly high. In the case of Enron, and in the case of Arthur Anderson, the consequences were catastrophic.

Fifth, when someone does commit an ethical violation, a company should move to fix the problem and remedy the harm as quickly as possible. It also has to take appropriate action against the offending employee - swiftly and firmly. It speaks volumes when a company fires or suspends a rainmaker or other important employee for an ethical breach; and just as importantly, it speaks volumes when a company doesn't. And as much as possible (and consistent with privacy concerns), the punishment and the reason for it should be clear to the company's other employees. Not too long ago, a company came in to tell us about some rule violations by a handful of employees. After applauding the company's decision to self-report, we asked whether the company had experienced any similar problems in the past. The company said that it had, but was quick to add that they had disciplined those employees. The problem, though, was that those disciplinary measures had been taken so quietly that the company had failed to convey to its other employees in a clear and forceful way that such conduct was unacceptable. Perhaps as a result, the company found itself having to deal with the same rule violations by a different set of employees. Setting the right tone means letting employees know that no one at the company is above the law; that no matter how important or how senior, someone who has violated an ethical standard will be punished.

Sixth, hold all of your managers accountable for setting the right tone. That means disciplining or even firing them when they have failed to create a culture of compliance. Human nature being what it is, there will be those who break the rules. But if managers don't do enough to prevent those violations, or let them go unaddressed for too long, then they should be held responsible - even in the absence of direct involvement in those violations.

Seventh, monitor, follow up and re-assess.

Cultivating a culture of compliance requires a sustainable effort. A one-time push is not enough. Employees will see such an effort for what it is and won't believe it represents a true commitment to an ethical culture. You have to make sure, on a regular basis, that your code of conduct and your policies and procedures are being followed. That means giving your internal audit and compliance functions the resources and tools they need to do their jobs. Examine data from complaint lines and your ombudsman to determine whether your company is living up to its values. And don't get complacent. It's easy to fall victim to the phenomenon of "creeping" non-compliance. Business practices can change incrementally so that - in the same way you might not notice someone growing old if you see that person every day - it might be hard to appreciate how far a business practice has changed since its inception. Try to look at business practices anew on a periodic basis; don't just assume that if a practice passed muster years ago, it's still okay. And by the same token, look at your compliance regime periodically to make sure that it still works for your business.

Eighth, and finally: Notwithstanding everything I've said, don't fall victim to a checklist mentality.

As Richard Breeden wrote from his perch as WorldCom's Corporate Monitor: "[I]n several areas, WorldCom exceeded the accepted norms of 'best practice' in corporate governance, even though there was little if anything about its governance that was 'good' in reality. This illustrates the fact that good governance is not achieved by simply adhering to 'checklists' of recommended 'best practices.'" In short, you need to think through these matters in light of your own company's unique issues and history and develop your own approach to doing the right thing and making the commitment to doing the right thing, part of your company's DNA. Use checklists at the end of the process to make sure you haven't missed anything. They shouldn't be the starting point.

Conclusion

I began my remarks by taking note of the actions the Commission has taken against a host of well-known companies and individuals. Those cases paint a generally grim picture of the recent state of American business culture.

I'd like to end my remarks, though, on a slightly more positive note. While I know our enforcement pipeline remains quite full, I do have the sense - albeit a somewhat guarded sense - that the lessons of Enron and WorldCom and the other cases we've brought in the last few years have begun to take hold. But we can't afford to be complacent. Once the recent scandals recede from our collective memories, it's corporate culture that will serve as the bulwark against the eruption of a new scandal. At another time and in another context, abolitionist Wendell Phillips said: "Eternal vigilance is the price of liberty . . . ." Eternal vigilance is sound advice in this time and in this context. By soundly endorsing the values of honesty and integrity, by rewarding employees who adhere to those values, and by providing avenues for employees to report ethical lapses, you can cultivate a healthy, thriving ethical climate in your companies. By setting a tone of integrity at the top, you can create a climate for long-term success, a climate in which everyone gets it right.

Thank you.

http://www.sec.gov/news/speech/spch120304smc.htm

LOOKING FOR RISK IN ALL THE RIGHT PLACES

Anonymous reporting is an undiscovered asset for internal auditors that helps them obtain a valuable view of enterprise risk.

ALICE PETERSON

Looking for a better way to proactively identify key risks in your organization? The knowledge is right under your nose.

Try as we might, we will never completely eliminate risk in our enterprises. And who would want to work in an organization with no risk anyway? No risk, no reward. The trick is to find ways to be as successful as possible working with the imperfect human beings who are so critical to achieving our missions.

Keeping risk front and center on the corporate agenda has had quantifiably positive results. The new generation of "hotlines" represents the latest tool in obtaining a well-rounded view of enterprise risk. It is a simple yet powerful notion: get employees to tell you about risky behavior (they know!), and consolidate the information into an analytical framework designed to identify and act upon trends. This is the essence of a well-conceived and well-executed anonymous reporting solution—one that provides real benefit to the internal auditor.

Managing risk starts with culture

It can be an elusive concept, yet any enterprise that wishes to be successful must care about its culture. In the business setting, culture is the totality of attitudes, values, and philosophies that drive the behaviors of individuals and groups. The leadership team must ensure that the cultural vision is being sold deep down into the organization. This is done by consciously setting examples—by resolving dilemmas ethically and consistently calling out deviations from the company's values, and ultimately by rewarding good cultural behavior and punishing bad.

Communicating integrity and transparency in daily word and action is a business basic. It is hard to find an enterprise today that does not say that it has an "open door policy." The notion is already quaint, as it hearkens back to the day when managers worked in offices with doors that could close. Of course, the expression refers to management being open to hearing about the world as it really is, and not just the way they want it to be. Today's "open door" must be open not only to rank-and-file employees, but also to senior executives, vendors, and even the board of directors. It is healthy to surface complaints, suggestions, disappointing results, and problems of all sorts.

While most managers would prefer to have bad news delivered in person, there are two major reasons why this does not happen as often as it should in most workplace cultures:

1. It is human nature to avoid a backlash that could be personally hurtful, and

ALICE PETERSON is the president of Syrus Global (www.syrusglobal.com), a provider of services that advance organizational ethics.

AUDITING AN ANONYMOUS REPORTING PROGRAM

It is a good idea to test the key facets of an anonymous reporting program each year. The evaluation process should be designed with the organization's unique circumstances and risk profile in mind. Below are key questions and audit steps that should be considered:

1. Do employees and vendors know about the anonymous reporting service?
   - Verify that posters are clearly visible in public employee areas, such as copy rooms, break rooms, and the like. Are they legible and easy to understand?
   - Confirm that the contact information for the outside reporting service is either included in vendor contracts or otherwise made available to key vendors.
   - Determine whether new employees are provided information about the service in their orientation materials.
   - Obtain statistics from annual employee surveys regarding knowledge and trust of the service.
2. Are the mechanics of receiving reports from submitters working properly? Test the toll-free domestic and international hotlines. To get a true test, actually submit hypothetical cases and track what happens.

Submitter's Perspective

- Was the website functioning properly?
- How quickly did your call get answered?
- Was the listener effective at probing for a full set of facts?
- Were you provided a case number or other means of continuing an anonymous dialogue?
- Did the service function as described in the poster and brochures?
- Did you feel your submission was confidential?
- Did the check-back mechanism work, via phone, Web, and e-mail?

as a result people are often afraid to speak out.

2. Many managers do not clearly show their employees that they really do want to know the whole truth.

People who have been in the workplace a while have likely worked for two kinds of bosses: the manager who does not value feedback (although this breed of manager is getting very rare indeed), and the manager who genuinely wants to know what is going on. There are fewer and fewer of the former, and the latter invariably prefer that employees walk right in and tell him or her face-to-face what is happening, including wrongdoing.

The direct approach allows managers to put the information into context, which helps them know what to do about it. However, sometimes the proverbial open door cannot open widely enough, and it is just too scary for people to come forward unless they can do so anonymously. If they have the chance to safely and confidentially report wrongdoing, they will. Clearly, organizations do not want the anonymous mech-

AUDITING AN ANONYMOUS REPORTING PROGRAM *CONT'D*

Management's Perspective

- **Did the test submission spawn the prescribed alerts?**
- **How quickly after the submission occurred did alert e-mails reach review team members?**
- **Were the appropriate categories and significance levels ascribed to the case?**
- **Did the Web portal for handling and tracking cases work properly?**
- **Was management able to supply a response to the anonymous submitter?**
- **Was management able to communicate with the rest of the review team for the case using the Web portal?**
- **Did follow-up submissions from the anonymous submitter show up in the case diary?**
- **Did the system of checks and balances work?**
- **Was input from two people from different reporting groups required to close the case?**
- **Was management able to analyze data effectively and produce meaningful summaries for senior management and the board?**
- **Was the bypass mechanism functioning?**

General Effectiveness

- **Is any group of employees not being heard from? (Over a two-year or longer period, you should expect to see a representative sampling from all levels and all areas.)**
- **Is the overall usage low or high? (At most companies, 1 to 2 percent of employees use the typical service annually. Neither a low nor a high usage percentage is cause for concern; understanding the reasons, however, is very important.)**
- **Is management responding in a timely way to submissions? (Responding faster to more significant cases is important, but responding to all submissions is also key.)**
- **What percentage of the time was no management response supplied at all?**
- **Are summary analyses being sent to the proper oversight bodies, such as the board of directors?**
- **Is the review team structure still appropriate?**
- **Has the review team structure been updated for management changes?**
- **Is management taking action that is commensurate with the issues identified?**

anism to become the routine way employees communicate with one another. It is most effective as a "failsafe," used only after more direct ways of communicating have been considered.

The best confidential reporting solution in the universe cannot make up for bad examples set by management, a culture of corner-cutting, and a lack of education about the locations of the corporate "lines in the sand." A confidential reporting solution operates like a keystone over an arch—it is essential to hold all the elements of an ethical culture in place to produce a functional organization. It is listening that allows you to address issues; not listening keeps you in the dark.

In May 2006, the Open Compliance & Ethics Group (OCEG) released an internal audit methodology for evaluating the effectiveness of ethics and compliance programs. In this practice aid, trusted anonymous reporting systems play a key role in establishing an open culture. "Employees must be required to raise and resolve violations of compliance or ethics standards. To do so, they must feel confident that they can take action without fear of retaliation. Such fears have been reduced, but not eliminated, with the introduction of the 'whistleblower' protections of the Sarbanes-Oxley Act and the Canadian equivalents."[1] Additionally, the aid points out that the existence of a hotline is not enough. It is crucial to have the processes and procedures in place to investigate consistently all issues raised.

What features and capabilities are ideal for internal auditors? What will help detect risk early on and help track outcomes?

Just installing a hotline won't cut it

If only it were as simple as calling the first company that appeared at the top of the Google search list for "whistleblower." Doing it right is considerably more involved. The internal auditing function should consider the following anonymous reporting solution must-haves. Some draw on the organizational culture and internal activities, while others are the domain of the independent service provider.

IF YOUR ORGANIZATION HAS NOT DONE A GOOD JOB OF REINFORCING THE TRUE SAFETY OF USING AN ANONYMOUS REPORTING MECHANISM, IT WILL BE REJECTED, AND VALUABLE INFORMATION WILL GO UNHEARD.

Trust. Without trust, an anonymous reporting mechanism will not be used. And if it is not used . . . well, why bother? The single biggest driver of trust is independence. It is difficult, if not impossible, to achieve the perception of true independence with an internally managed hotline. Some leaders are quick to say, "Our own people know our business better than anyone else. We will be able to ask better questions of the submitter than a third-party provider could." Similarly, some believe that sensitive information is best kept out of the hands of an outsourced service.

Empirical evidence indicating otherwise is compelling: Internal hotlines do not get used as readily as external ones, and they are particularly at risk for not surfacing information from mid- and senior-level associates. Outsourcing anonymous reporting to an independent and experienced firm is the first important step in ensuring that it will be trusted.

It also helps to have no employer presence indicated when the submitter uses the service. For example, when an Acme employee calls the tip line and hears "Acme hotline," he or she is likely to question the independence. Likewise, when an Acme employee uses the Web option for reporting, and the first thing seen is the Acme logo, he or she is likely to be put off. With both of these situations, Acme will experience abandonment.

Outsourced, and thus independent, services lose some of their trust-value when companies insist on a vanity toll-free number that spells the company's name, or make similar requests. Establishing the independence of the reporting solution is the secret to getting the best results. You might be just about to convince the anxious Acme submitter to call the hotline . . . until he sees that the number he is supposed to call is 1-800-AcmeTips.

Enterprises with independent listening services in place often thwart their own efforts by commenting in front of employees, or indicating by their behavior, that they would prefer not to get reports from the service. Doing so can instantly dash an anxious submitter's trust in using an anonymous reporting service. A company's employees should know unilaterally that the company will never attempt to discover the identity of an anonymous submitter.

Here is an example of a typical path that an employee travels before using an anonymous reporting mechanism:

> "I could tell my boss about this terrible thing, but I'm not sure she would take it in the constructive spirit in which I'm offering it. I could go to my boss's boss, but if my boss found out, I'd be dead for sure. I could go to human resources, but I can't trust that it wouldn't backfire somehow. Even if the management here didn't retaliate in some way immediately, the retaliation could occur in the future or in subtle ways . . . and I'd never know when or how."

The fear is very real, and real lives are affected by the aftermath of "whistleblowing." The person who has something to report has already considered the alternatives. If your organization has not done a good job of reinforcing the true safety of using an anonymous reporting mechanism, it will be rejected, and valuable information will go unheard.

CALLERS OFTEN DISCLOSE MORE THAN WHAT THEY ORIGINALLY INTENDED TO REPORT WHEN THEY SPEAK WITH A SKILLED LISTENER.

There is often a misconception that anonymous reporting solutions are an outlet for lower-level employees only. You want to hear from employees at every level if there is a known problem; the old adage, "big people, big problems" is true in many ways. It is imperative to go the extra mile to make the high-level employee comfortable that even where the air is thin, he or she will be protected from retaliation for his or her whistleblowing.

For many services, "confidentiality" simply means asking "Do you wish to remain anonymous?" at the beginning of the call. This is insufficient protection for, and no comfort to, the anxious submitter, particularly if he or she is a high-level employee or business partner.

An effective anonymous reporting solution is one that is trusted by all levels of employees and even by the organization's vendors and partners, who should also use it when they are aware of corporate malfeasance.

Ease, control, and choice are other elements of trust. Let submitters know they can choose how they communicate with your outsourced service—a toll-free phone number, a secure Web portal, a post office box, etc. Also, let them drive the process. As soon as an employee feels that you are making him or her do it "your way," he or she might recoil or even abandon the attempt.

An example of how submission methods can frustrate employees is a Web-based form full of boxes to complete; a submitter can get exhausted just looking at all the empty spaces and give up. The process for submitting reports via the Web should be designed to be hassle-free and freeform. Submitters should not be burdened with someone else's idea of what to put in which text box.

Look for an overall submission design that makes it easy for the submitter to contact you; too often, service providers design the approach in a way that simplifies their effort, rather than that of potential submitters.

Phone services should always let the caller tell his or her story, his or her way, without a lot of up-front information collection. Faced with scripted, required questions, callers may despair about the true confidentiality of the call, feel a loss in control, and ultimately may "chicken out" entirely.

Complete information capture. Obtaining critical discoveries from submitters is a way to turn an anonymous reporting program into a real competitive advantage for your organization.

The phone call is a golden opportunity to engage in a two-way dialogue and get a full set of facts. The fuller the set of facts, the better the company knows how to address the issue, which saves time and money. It is key to have educated professionals taking the calls—someone who can put the caller at ease, gently probe for important facts, separate fact from emotion, pick up on innuendo, and find out what is really going on. When the listener is unskilled and does not have the tools to optimize the outcome, you will get only the most basic who-what-where information. Callers often disclose more than what they originally intended to report when they speak with a skilled listener. Thoughtful, personal discourse is a great way to pick up all the "little things" that may not seem significant by themselves, but when accumulated become a great early warning signal that allows management to tackle issues before they fester.

My organization's listening service once heard from a caller who reported that "the boss" was stealing. After going through a thorough investigation of the matter, we discovered that the stealing had been occurring for several months. More probing turned up the reason that sparked the call: "the boss" had decided that very morning that the caller's previously approved family leave could no longer be accommodated because of recent new contract work at the plant. In this particular circumstance, the denial of the leave was illegal, and thus a very important facet of the case to uncover. Without a freeform and unscripted conversation with an experienced, well-trained listener, important learning can go undiscovered. (We later learned that what the caller considered to be "stealing" had been discussed, approved, and known about by "the boss's" superiors.)

An essential element for complete information capture is the ability to continue the dialogue between the anonymous submitter and management. The simplest arrangement is generally to provide the phone and/or Web submitter with a case number identifying the confidential submission. The submitter is then informed that he or she can use the case number to check back to find out what management did or said as a result of the report. The capabilities for phone and Web submitters should be interchangeable. Even if the original submission was via phone, a submitter should be able to check back via the Web to see what management's response was, or to hear the follow-up questions that management would like answered in order to investigate.

It is important for a submitter to get feedback, even if management simply responds with, "Thank you. We appreciate that you came forward with this information."

Collect it all in one place. A nice feature provided by a few anonymous reporting service providers is a "direct entry" capability that allows companies to add directly reported and internally identified issues to the confidential database. Internal auditors identify issues in the course of their operational audit work. Human resources staff members pick up hints of problems and are able to directly deal with violations here and there. The risk management staff members hear about safety and security problems continuously. Employees wander into their managers' offices every so often to discuss ethical dilemmas and inform them of hot spots. And confidential employee reporting mechanisms can bring issues to the forefront up, down, and across the organization every day.

INTERNAL AUDITORS SHOULD BE GRANTED ACCESS TO ALL CATEGORIES OF DATA, WHETHER OR NOT THEY PLAY A ROLE ON THE REVIEW TEAMS.

With a direct entry option in an anonymous reporting solution, a company chooses which staff member is granted permission to directly enter cases into the master system. Multiple people can be provided the direct entry capability, or direct entry can be confined to a single person. People with direct entry responsibility need not be the same people who are charged with handling confidential reports.

Perhaps no single report alone sounds the big alarms. Maybe it all seems like small stuff in each respective area. But when you put the pieces together and look at the patterns that emerge, sometimes a different story takes shape.

Intelligent delivery. The right people must be informed about anonymous submissions on a timely basis, and e-mail is not the best way to accomplish this. A Web portal provides the ubiquitous access, the control, and the information security required. E-mail is inherently insecure, and you certainly don't want a "forward" button adjacent to sensitive information.

Establishing how confidential complaints will be handled is critical. Overall, the most desirable process includes transparency (among a defined number of people), controlled access, speed, ability to handle complexity, and flexibility.

Getting the right eyes on each report in a timely fashion is best facilitated through the use of a Web-based application service. After a case report is received, whether it comes via phone, Web, or letter, it needs to be categorized and prepared for delivery to the client's database. Ideally, each member of a company's "review team" should receive an automatic e-mail alert whenever something notable occurs in the client's database. This gives the review team members a "heads up" to log into the company's Web portal and read a new case or review a new activity.

Insist on processes that incorporate checks and balances to ensure that issues are not "swept under the rug." Depending on the size and complexity of the company, it can be desirable to have a different team handle different categories of issues. Exhibit 1 shows a sample review team matrix for a hypothetical company. Notice that each of the teams in this example has a "primary" handler and a "secondary" handler, each from different departments. A manager and his or her subordinate would not provide the desired checks and balances.

In this example, accounting and finance matters will be addressed by a team made up of internal audit and the ethics officer/general counsel; the ethics officer/general counsel and the head of human resources will handle discrimination and harassment issues; the head of retail operations (this could alternatively be the head of safety and security) and the head of

WHEN PEOPLE ARE AFRAID, THEY HESITATE TO TRUST THE CONFIDENTIALITY OF A SERVICE; THE ONUS IS ON MANAGEMENT TO GO ABOVE AND BEYOND TO REASSURE SUBMITTERS.

human resources will handle safety issues; and so on.

Internal auditors should be granted access to all categories of data, whether or not they play a role on the review teams. This allows them to stay abreast of issues as they are reported, to slice and dice the data periodically to look for trends, and to help set the audit priorities for the coming period.

Another key piece of the process is a "bypass" notification review team concept. Should senior management and/or the general notification review team members be alleged to be involved in serious wrongdoing, the bypass team receives the case report. Typically, the bypass team is comprised of independent company board members.

Every organization is unique, and it is important to establish flexibility for who sees what and under what circumstances. Ideally, one individual will be assigned as the single point of contact for the anonymous reporting service provider. In many cases, the single point of contact is either the ethics officer or the head of internal audit for the company. The single point of contact is responsible for setting up and granting permission to the database of ethics reports.

Strong follow-up and oversight processes. Making sure that the appropriate action is taken following the case submission is "where the rubber meets the road." Historically, many companies have had no way, or limited ways, of tracking and following up on confidential reports. In the past, reports often became buried in piles on someone's desk or were tossed out without proper attention, and it was often impossible for overseers to do their jobs because there was no methodical tracking of the actions that resulted from the reports received.

As the saying goes, "What gets measured gets done." It is necessary to have disciplined processes in place to ensure that issues are handled appropriately, and at the same time help managers weave these processes easily into their other daily responsibilities. As discussed, intelligent workflow services can provide for multiple review teams assigned to different types of submission categories. Other critical features of a robust tracking and handling system are keyword search capabilities, trend and pattern identification, and categorization of cases from any source—hotline, helpline, Web submission, or directly reported to a person—into a single database for the strongest searching, reporting, and predictive capabilities.

A best-practice tracking system resides on the outside service provider's servers, and is accessible via the Web 24 hours a day. The review team members, and everyone who has access to the data, are able to use the single system from anywhere in the world to take action and collaborate with the rest of the team. For example, the primary handler can use the Web portal to:

- send a management response;
- view a complete diary of all activity on a given case;
- add notes to the diary for the whole team to see;
- add personal notes that only they see;
- enter a resolution for the case; and
- analyze the data.

Analysis and reporting functions are critical to get the maximum benefit from the confidential reports. Internal auditors should periodically analyze the report data and ask hard questions, like whether or not certain business units are reporting control issues or weaknesses.

The payback on the initial investment in obtaining the expertise and tools of an anonymous reporting solution provider is tremendous not only in terms of opportunity cost, but also in terms of learning critical information that can make a difference to the future course of the company.

Spread the word about your third-party listening service the right way

A transparent organization consistently reminds its employees and partners—through posters, fliers, wallet cards, brochures, messages from the CEO or president, all-staff meetings, and reminders on pay stubs—that the company wants to know what they think and is listening to what they have to say. There are myriad ways to get the message across, but none is better than stating the case in public forums. Corporate leadership should always assure employees that the "open door" philosophy is alive and well and encourage employees to come forward on an identi-

EXHIBIT 1 Sample Review Team Matrix

General Notification Review Teams

Team Member	Acct'g & Finance	Corp. Waste	Discrimination	Fairness	Harassment	Legal	Regulatory	Safety & Security	Unethical Dealing	Suggestion	Other
Rueben Antoine Dir. of Internal Audit	Primary	Primary				FYI					
Michelle Chabert Chief Ethics Officer	Secondary	FYI	FYI	FYI	FYI	Secondary	Secondary	FYI	FYI	FYI	FYI
Yolanda Jackson VP, HR			Primary	Primary	Primary		FYI	Secondary	Secondary	Primary	Primary
Randall McKinney CFO	FYI	FYI							FYI		
Heidi Meyerson VP, Gen. Counsel	FYI	Secondary	Secondary	Secondary	Secondary	Primary	Primary	FYI	Primary	Secondary	Secondary
Roberta O'Brien Sr. VP–Retail Ops.								Primary			

Bypass Notification Review Teams

Team Member	Acct'g & Finance	Corp. Waste	Discrimination	Fairness	Harassment	Legal	Regulatory	Safety & Security	Unethical Dealing	Suggestion	Other
Pete Teasdale Chairman	FYI	FYI	FYI	FYI	FYI	FYI	FYI	FYI	FYI	FYI	FYI
Nancy Wu Audit Comm. Member	Secondary	Secondary	Primary	Secondary	Primary	Secondary	Primary	Secondary	Primary	Secondary	Primary
Jim Young Audit Comm. Chairman	Primary	Primary	Secondary	Primary	Secondary	Primary	Secondary	Primary	Secondary	Primary	Secondary

fied basis to report news or make suggestions to improve the enterprise on an ongoing basis.

Leaders should regularly reinforce the company's policy of non-retaliation. In the same breath, they should acknowledge that anyone uncomfortable with the "open door" path may choose to make an anonymous and confidential report. This permission to use a third-party listening service is the outlet some employees need to feel comfortable about reporting malfeasance.

Employees should know that management will not attempt to learn the identity of anonymous submitters. This pledge should be included in every message that announces and communicates the service, including brochures, posters, e-mails, and so on. Put the pledge on posters in the lunchroom. Put the pledge in the code of conduct. Make sure every employee knows it.

When people are afraid, they hesitate to trust the confidentiality of a service; the onus is on management to go above and beyond to reassure submitters. Choose your anonymous reporting service wisely, and such assurance is within reach: the finest ones have carefully trained people read every confidential submission and put themselves in the shoes of the submitter to remove any inadvertent clues to identity. Suppose a submitter says, "I'm sure the second time I witnessed the theft was March 14, because that was my 40th birthday, and. . . ." The fact that it was March 14 is important. The fact that it was the submitter's birthday is not necessary for the pursuit of a logical investigation and its ensuing action. Slashing through "that was my 40th birthday" in the case report helps management, as they cannot "un-know" something that has already been revealed to them, and they want to hold up their end of the "won't attempt to learn identity" bargain.

Telling employees how far you and your service partner go to protect their anonymity is impressive, and it is what people need to hear when there is extreme anxiety about revealing problems (especially when the submitter has become complicit in the act, which happens frequently). Publicize the specific processes that demonstrate that the third-party reporting service keeps submitters safe.

Working with the audit committee and the board of directors

Today's board wants to know what is really going on. What management team does not want to look as good as possible? It is the responsibility of the board to obtain objective information from a variety of sources, not just from management, and the case management system can be a great source of unfiltered information from the front line of the company. The sophisticated service will aggregate information into high-level reports for directors, with the ability to instantaneously drill down to the detail when it is of interest.

The board will want to have a couple of investigation firms pre-cleared and the relevant contact information at the directors' fingertips. In the unlikely and infrequent circumstance where a high-level issue needs to be looked into by professionals, the board will want to jump on the issue without delay. (Likewise, management should have a plan on internal investigations mapped out in advance.)

A best practice is for all board members to have a login and password to the anonymous report database and for them to visit the site periodically to see what employees are saying about the company. It is essential that the audit committee's chairman has "anytime access" to the confidential communication from employees. Alternatively, a summary of highlights, ideally using graphics to allow for the most efficient review possible, can be uploaded to the board's extranet, or wherever essential board materials and other information are held electronically. Board members who know what employees are saying confidentially are in a better position to ask insightful questions and work to improve the outlook for shareholders.

The board of directors should oversee the features and capabilities of the anonymous reporting solution, and should review annually the processes for case management. Internal auditors should test the service annually and report any shortcomings to the audit committee.

Anonymity and confidentiality are necessary prerequisites to ensure a comfort level, and this goes for all employees, from the assembly line workers to senior management. Even in companies where the "open door" is working well, an option for confidential communication at all levels is an essential adjunct to a confidential communications program. By enabling anyone anytime to report something safely, management and boards can tap into "the water cooler" and can better operate and oversee a well-run enterprise.

Conclusion

A comprehensive anonymous reporting system can do a lot of internal audit legwork for you. In addition to serving as a repository of issues identified anonymously, other issues from audits and those identified internally may also be logged and tracked in the same system. This approach not only provides you with a snapshot of enterprise risk, it can also show you how well or poorly your organization is managing these risks. It can provide you with a safe and secure way to monitor ongoing case management. And, it offers a way to easily and efficiently communicate your findings with your audit committee members. When looking for risk, remember that internal auditors need to know what employees know. ■

NOTE

[1] Open Compliance & Ethics Group, *Internal Audit Guide: Evaluating a Compliance and Ethics Program,* exposure draft issued May 2006: 8.