WHITE PAPER

The High Cost of Non-Compliance: Reaping the Rewards of an Effective Compliance Program

RICHARD M. STEINBERG

FEBRUARY 2010

OPENPAGES

Clarity. Confidence. Control.

Table of Contents

About OpenPages®: OpenPages is the leading provider of integrated risk management solutions for global companies. The OpenPages Governance, Risk and Compliance (GRC) Platform empowers a risk-based approach to identify and manage key business risks across the enterprise. This approach enables companies to focus on what's important and to avoid unexpected outcomes while improving performance. Founded in 1996, the company is headquartered in Waltham, Massachusetts, with international offices in the United Kingdom, distribution partners in Japan and South Africa and regional offices throughout North America.

For more information call 781.693.5999 or visit us online at www.openpages.com.

The information presented here does not constitute legal or other professional advice. Companies are encouraged to consult legal counsel concerning their responsibilities for legal and regulatory compliance.

Executive Summary

Companies are finding legal and regulatory compliance costs soaring while effectiveness declines, giving rise to huge fines, penalties, awards and settlements — often in the billions of dollars. Policies and procedures build with each new law and regulation but are disparate, duplicative, and fail to comprise an effective compliance program.

Some companies not only have made their programs effective and efficient, but also gained tremendous business benefit. Understanding the rationale for ever expanding legal and regulatory requirements, they recognize the underlying marketplace drivers and align strategic initiatives to gain market share, profit and return.

By aligning business objectives and building compliance programs into existing management and business processes, responsibility and accountability is put where it works best, increasing effectiveness, reducing cost, and providing senior management and the board with the information they need.

What's the state of your company's compliance program? Is it truly effective, and are you satisfied with its costs and benefits? Have senior executives in your organization said things like:

- "We're fine, because we've never had a major compliance problem."
- "The kinds of problems our peers suffered couldn't happen here — we're better and smarter than that."
- "We already have a code of conduct, whistleblower channel, and other elements of what's required for compliance."
- "Our general counsel has responsibility for ensuring we're fully compliant with all laws and regulations, so we're covered."

If you're an experienced compliance professional reading this, you're probably cringing at these "positive" expressions of satisfaction. But whatever your corporate responsibilities, if you're concerned about the cost and effectiveness of your company's compliance program, please read on.

The Back Breaking Costs

Leaving program effectiveness for a bit later, let's take a look at the tremendous costs of dealing with compliance — which can be viewed similarly to those automobile motor oil ads of long ago — "you can pay me now, or pay me later" — a few dollars now, or thousands later, although here, the later numbers are much larger.

Cost information varies based on any number of surveys, but they provide at least directional insight. One survey of several years ago shows for every $1 billion in revenue, the cost of compliance programs comes close to $6 million.[1] Another shows the cost of Sarbanes-Oxley compliance alone averaging $4 million for companies with $5 billion revenue, and $10 million for companies with $10 billion and more in revenue. More telling is that for companies with more than $1 billion revenue, compliance costs equaled 190 full time equivalent employees.[2]

And when we consider one of the highly regulated industries — the U.S. securities industry — compliance costs for each firm averaged a whopping 13 percent of revenues.[3] And this is of course before the near financial system meltdown and legislative and regulatory reaction now under way.

When looking at the cost of a compliance failure, the numbers take on even greater significance. The later study found that $1 billion revenue companies having just one compliance failure incurred $81 million in costs — consisting of settlement fees of $64 million, lost business of $14 million, and fine, remediation and business interruption of $3 million.[4]

Unfortunately, those numbers pale in comparison to compliance failures suffered by many companies — each running in the billions of dollars. Looking at just a handful of those companies, media reports show the following payouts:

- American Home Products — diet product — $3.75 billion
- Bank of Credit and Commerce — fraud — $17 billion
- BAT Industries — tobacco settlement — $73 billion
- Cinergy — pollution - $1.4 billion
- IBM — age discrimination — $6 billion
- Johns Manville — asbestos — $3 billion
- Philip Morris — tobacco settlement — $9 billion
- Prudential Insurance — sales practices — $4 billion
- Texaco — interfering in merger — $3 billion
- Time Warner — accounting practices — $3.5 billion
- Visa — anticompetitive business practices — $2.25 billion

Loss of market capitalization often is dramatic, with examples including Merck's Vioxx product liability cutting $40 billion in market cap and Marsh's bid rigging causing a reduction of over $10 billion.[5]

So, while implementing a compliance program may seem high, it's clear that not putting an effective compliance program in place can be significantly more expensive. The already high and growing cost of complying with laws and regulations to which companies are subject has gotten the attention of senior management and the board of directors. Drawing significant focus is the reality that while costs continue to rise, the effectiveness of compliance programs doesn't necessarily keep up and may in fact deteriorate. So, with costs becoming virtually unsustainable in the context of other business pressures, senior management teams and boards are looking at ways to make compliance programs both more efficient and effective.

Beyond the Direct Costs

We should make no mistake — compliance is up there with strategy and risk management in boardroom discussions today. As noted, it's not just the significant costs, but program effectiveness that has captured attention, for good reason. Directors are well aware of the myriad laws and regulations to which their companies are subject. As a brief sampling, these include broadly applicable requirements related to product safety, employment, workplace health and safety, employee benefits, pensions, securities laws; those cutting across a number of industries dealing with information privacy, anti-money laundering, and appropriateness of product to customer profile; and industry-specific mandates for government contractors, pharmaceuticals, and health care, tobacco and telecom companies.

Just as eye-catching are enforcement and related regulatory actions for noncompliance. These include ongoing and renewed activity by the Securities and Exchange Commission and Department of Justice, each of which is known to take a "carrot and stick" approach — being more lenient where a compliance program is strong, and tougher enforcement when it is not. Then there are the Delaware Chancery and Supreme Court cases which underscore board responsibilities for ensuring effective compliance programs. Also having gained critical notice are the federal sentencing guidelines which deal with criminal misconduct and company's programs for assessing and reducing the related risks.

Experienced directors know well that a major compliance failure can not only cost billions of dollars in direct costs, but also bring a company to its knees. At a minimum, it steals time and energy of top management, detracting from day-to-day running of the company and new initiatives to grow the business. And damage to a company's reputation, which takes years to develop and can be destroyed overnight, affects relationships with customers, suppliers, alliance partners, bankers, and investors, as well as retention of key human resources and ultimately long term success.

How We Got Here

To see the best way forward, it's worth taking a quick look at some of the factors that caused companies to get to the untenable position many are now in.

- Companies typically have in place a number of policies and procedures directed at legal and regulatory compliance,[6] including a code of conduct, whistleblower channel, educational programs, and annual employee sign-offs. In large companies, sometimes depending on the industry, there is a designated chief compliance officer and staff, whereas in others the general counsel or other corporate lawyer serves in the role. But too often these are disparate elements that fail to function effectively as a true compliance program.
- Also typical is a build up over time of layer upon layer of policy and procedure, each dealing with various aspects of legal and regulatory requirements. For each new law or regulation, new internal procedures are designed to deal with specifics of the rule. Unfortunately, often each is free-standing without considering existing protocols in the organization that may already address the new requirements.
- Responsibility for compliance rests with one senior manager. From the perspective of a company's chief executive, it's desirable to be able to look to one individual with the authority and accountability to achieve desired performance. This of course holds for business operations, as well as for such areas as finance, technology, human resources, and so forth. Responsibility for compliance is placed with the company's general counsel or chief compliance officer, where this individual is charged with ensuring the organization adheres to all legal and regulatory requirements to which the company is subject. This approach also is embraced by boards of directors that see benefit in such central assignment of responsibility. While in some respects appealing, reality is that this approach places responsibility for effecting compliance in the wrong place.
- Another factor is viewing compliance as a necessary evil, and a costly one at that. Certainly, the thought goes, it's a drain on resources that could otherwise be used to grow the business and enhance profitability. This philosophy, however, can be counterproductive from a business perspective.

Keys to Getting it Right

Some companies have avoided these pitfalls and succeeded not only in reducing compliance costs, but also enhancing efficiency and gaining real business benefit. Let's look at how they've succeeded in getting this right.

- **Strategic Perspective.** Moving from seeing compliance as a costly but necessary evil, forward looking management teams see the bigger picture, beginning with the realization that new laws and regulations arise from corporate actions that caused damage — to consumers, employees, investors or the community. Each legislative or regulatory reaction raises the performance bar in such areas as product safety, human resource discrimination, information privacy and security, the environment, sales practices, and financial reporting. These insightful corporate leaders recognize that despite raising of the bar, the marketplace sees these new standards as a minimum, with consumers looking for those products and services that meet their higher expectations.

Successful managers "get it," and their companies reap the benefits in terms of market share, profitability and return. One can look to the auto manufacturer that has long been a leader in gaining better mileage performance, or another that has been a leader in vehicle safety. Companies that recognized the demand for healthier food products — both retail and restaurant based — have gained market share. And an airline instituting a passenger "bill of rights" continues to achieve high customer satisfaction ratings, gain market share and lead competitors in profitability. Companies with fair and forward looking HR programs attract and retain the best personnel, and those with reliable and transparent financial reporting are viewed by the investor community as lower risk resulting in lower cost of capital. These companies recognize that legal and regulatory requirements indicate a demand for better performance, and have met the challenge by exceeding minimum requirements.

- **Built into Business Processes.** Recognizing the underlying motivations behind legal and regulatory requirements and related marketplace expectations, forward-looking companies align their compliance process with the company's business goals and objectives, and build it into its existing business processes. As such, responsibility for compliance rests not with a compliance officer, but rather with each and every line and staff manager in their spheres of responsibility.

  Yes, a chief compliance officer is critical to ensuring a compliance program is well designed and provides the necessary support to the management structure for its implementation. This responsibility includes ensuring what often are disparate elements are crafted into a cohesive compliance program. More on this in a moment.

  The take away point here is that administrative costs soar if compliance is superimposed on top of existing procedures. When built into the management process, compliance is both more effective and efficient. Looking at one simple example, a broker-dealer seeking to comply with requirements for use of current marketing materials for customer proposals added costly monitoring procedures from an independent compliance group. Another, however, placed responsibility with local sales managers — who are closest to the "action" and know well what materials are being used by local sales personnel. Not only is compliance more effective — better ensuring use of current materials and meeting clients' expectations for quality service — it is also more efficient, even when accompanied by ancillary monitoring on a test basis by compliance or internal audit personnel.

- **A Program Founded on Ethics and Integrity.** To be truly effective, the compliance program must be grounded in a culture based on integrity and strong ethical values. A company's culture is based first and foremost on the actions (more so than, but including, the words) of top management as well as managers cascading throughout the organization. Without integrity, a compliance program will have form but not substance, and over time will fail to do what it's designed to do.

Central to an effective compliance program is an ethics policy designed to meet the activities and culture of the company. The policy needs to be sufficiently comprehensive, but also organized and written to be understandable, and readily accessible as needed to deal with day-to-day real life issues. The same holds for all policies, which need to have a business owner and be kept current and responsive to changing conditions. A recipe for disaster is having policy material that is too long, written in legalese, outdated and hard to locate — such that non-compliance is virtually assured.

With integrity as a hallmark, a compliance program must engage the company's employees. They need to understand the reasons behind the rules — for the benefit of the company, its personnel, customers, and others. Reality is that employees who don't know why they're supposed to do something will go through the motions with a checklist mentality, if at all. So, educational programs should be in place — not just upon hiring, but ongoing — coupled with on-the-job reinforcement by unit leaders.

With whistleblower channels in place — dealing with any potential wrongdoing, not just what's required by Sarbanes-Oxley — personnel need to know that using those channels is fundamental to a culture of integrity and ethical values, and is in the company's best interest and their own. The channel needs to be truly user-friendly, such that there is no uncertainty in reporting any concern, with an ombudsman or other support personnel ready to answer questions and facilitate communication. And of course, appropriate follow up action with no possibility or concern of reprisal is a key.

- **A Risk-Based Approach and Clarity Around Responsibilities.** Companies sometimes set a "zero tolerance" approach to compliance, which indeed makes sense from a mind-set perspective. Ignoring small wrong doings can send an unintended message that compliance isn't really important. With that said, reality is that some rules carry more significance than others, and resources always have limitations.

  Accordingly, risks need to be identified as to where and how non-compliance can occur and the likelihood of occurrence and impact on the company if it does. And with needs targeted, resources need to be placed where they will do the most good, bringing the risks down to acceptable levels.

  As noted, responsibility for compliance is best placed with line and staff managers who run operating business and staff functions. This involves more than simply assigning responsibility. It also distinguishes design, execution and monitoring activities, including interfaces between operating and support units and the compliance and central monitoring functions, and clear handoffs with overlaps avoided. With roles understood and built into HR processes, accountability can be established and performance measured over time.

- **Technology.** For mid-size and large organizations, central to an effective compliance process is sound use of technology. Done well, IT facilitates such matters as ensuring the code of conduct and other relevant policies are readily accessible, supporting the ongoing education process, facilitating employee certifications, and providing a user-friendly means of providing information or addressing concerns regarding potential non-compliance.

  Recognizing that the regulatory environment continues to increase in complexity, leading organizations have moved away from manual based methods for compliance, deploying technology to centralize and manage the full range of compliance activities. As a critical enabler, technology supports established compliance management process and methodology, but does not define them. Among the benefits are:

  – Providing real-time data management and decision support to ensure that senior management and the board of directors receive accurate information on causes, financial impact, and mitigating actions to control risk of compliance failures

  – Enabling policy lifecycle management to create, approve, maintain, store, monitor, and automate tasks based on company policy requirements

  – Delivering policy training and awareness, surveys, and related testing feedback

  – Establishing automated workflows to establish employee accountability

  – Automating and streamlining processes and information retrieval, including control testing, surveys, certification and regulatory reporting

  – Supporting measurement and reporting through a central repository of policies, procedures, risks, and controls

  These capabilities are used to fix responsibilities for required actions by managers or monitors, and to track activities and enable inquiry from and to senior personnel. Real-time messaging and reporting capabilities provide the necessary information for use throughout the managerial ranks and the compliance function, with tailored dashboards and drill-down capability to home in on matters of particular interest.

- **Strong Compliance Office.** As noted, critical to effective compliance is a designated chief compliance officer, who depending on the company's industry and size can be a part-time position or full-time with dedicated staff. This individual must ensure all the necessary pieces are in place and brought together to be truly effective.

  For instance, managers in the organization must receive information on existing and new laws and regulations relevant to their operational responsibilities. They all have "day jobs" and can't be expected to know what's required, unless the legal or compliance function provides them with needed information in a form that's easily implemented. Importantly, the compliance officer needs to be sure any new requirements are considered in the context of existing procedures, to avoid adding unnecessary layers. In many instances, existing protocols may already address new rules, or require only minor tweaks to get them where they need to be. Overreaction can be as debilitating an under reacting, as scarce resources are wasted on unnecessary procedures.

The compliance officer must ensure close coordination between the various activities that drive compliance, including monitoring of program effectiveness with the internal audit function, and interface with legal counsel (if separate from the compliance office) and top management.

And the compliance officer can promote and facilitate communication throughout the organization. For instance, messages on integrity need to be ongoing and reinforced. Information on potential issues of non-compliance must be communicated through regular managerial routes or separate channels, such that appropriate action and follow up can be initiated. And information needs to flow not only up and down the organization, but across as well, changing what might be a silo mentality into one where managers at every level throughout the company communicate as needed.

In this context, there needs to be clear and timely reporting in meaningful form to top management and ultimately the board of directors. Metrics on instances of non-compliance, along with severity and patterns and underlying causes, are needed to enable inquiry and corrective action. Reporting of course should become more summarized going upstream, although enough depth is needed to allow full understanding.

Making it Happen

How do you move to the desired compliance process? The way is straightforward, though as with any change initiative there are potential pitfalls.

Among the tried and true approaches is a multi-step sequential process that looks at what currently is in place, determines where you want to be, and crafts an action plan for getting there. Also important is dealing with senior managers who might want limited resources devoted to other important business initiatives. With that in mind, here's a brief outline of what experience shows works well:

1. **Make the business case.** Get a rough estimate of current costs involved in dealing with compliance matters, including the risks and costs associated with non-compliance events. Relate this to a streamlined process built into business operations, together with support personnel and the cost of the change initiative. It's important to include the benefit of enhanced program effectiveness and anticipation of fewer and less costly non-compliance events, and the ability of senior management and the board to have better information and greater comfort. Because CEOs and boards usually already recognize shortcomings of existing compliance efforts, usually there is good receptivity to thoughtful rationale for building a truly effective and efficient compliance process.

2. **Assess where you are.** Consider the "current" or "as is" state, including an inventory of compliance policies and procedures — both written and unwritten — and authorities and support functions to get an in-depth understanding of the compliance activities.

3. **Design the desired process.** The "future" or "to be" state is developed. Importantly, design must reflect the corporate culture, including such factors as the organization structure, management style, and other embedded cultural features reflecting the desired tone at the top based on a foundation of integrity and ethical values. In this context and as discussed above, the compliance process is designed to be built into the business and management processes, with established responsibilities, accountability and communication protocols. The process is principles- and risk- based, with details of specific procedures left to managers throughout the organization who will have operational responsibility, developed with support of the compliance office. Consideration also is given to such associated parties as outsource organizations, third party networks, alliance and joint venture partners, and merger or acquisition targets, whose actions can affect how the company is perceived and held accountable.

4. **Establish communication, reporting, monitoring.** Critical information flows are established — with needed two-way communication — along with capturing analyzed data for upward reporting to senior management and the board. Technology support is selected, tailored as necessary, and embedded to enable risk analysis, accountability, and communication. Monitoring protocols are established, with clear responsibilities among the compliance office and internal audit function and their interfaces with line and staff units.

5. **Roll-out and implementation.** The newly designed process is rolled out to the business, either starting with selected units or broadly across the enterprise. Training and education are critical, along with change management techniques to ensure employees fully understand what is needed, and why — that is, how new protocols will benefit every unit and the company as a whole. Personnel must truly buy in, coupled with integration into HR objective setting and performance assessment processes. Because compliance is built into existing business and management processes, new responsibilities are brought to the fore within the management structure in individual units, making implementation relatively straight forward.

The Rewards

Change is never easy. For most companies, however, continuing along the same compliance path is not a viable option. Costs are soaring, instances of non-compliance rising, and the risk of a devastating failure all too real.

Getting to a truly effective and efficient compliance process is attainable. Some companies have already gotten there, realizing the tremendous associated business benefits in understanding that the marketplace — consumer, work force, investor and societal — sees legal and regulatory requirements as a minimum standard, which when exceeded significantly enhances market share, profitability and return.

When one considers the current costs and lack of effectiveness, together with the upside potential, a decision to get this right becomes evident. Those companies that do get it right position themselves to reap the associated rewards.

About the Author

Rick Steinberg is CEO of Steinberg Governance Advisors, Inc. in Westport, Conn., where he advises boards of directors and senior executives of major multinationals — as well as large and middle market companies — on board responsibilities, governance best practices, and compliance and risk issues.

Steinberg previously was a senior partner at PricewaterhouseCoopers, where he served as the firm's corporate governance practice leader. He also was a founder of the firm's risk management and control consulting practice, and served as its global leader.

A sought-after speaker, Steinberg has authored numerous highly acclaimed reports, including Corporate Governance and the Board—What Works Best and its companion, Audit Committee Effectiveness —What Works Best. He also served as the lead project partner in developing the COSO Internal Control — Integrated Framework, now recognized as a landmark representing the standard of internal control, and played a similar role in the COSO's Enterprise Risk Management — Integrated Framework.

Steinberg is frequently quoted in the financial press and featured on national TV financial news programs, and has guest lectured at leading business schools. He has served as a member of the Conference Board's Global Corporate Governance Research Center Advisory Board, he is a member of the Open Compliance and Ethics Group Executive Advisory Panel, and is a member of corporate advisory boards. He is also co-founder of the Directors' College, presented by PricewaterhouseCoopers and the University of Delaware Center for Corporate Governance.

[1] OCEG 2005 Benchmarking Study

[2] META Group research conducted on behalf of PricewaterhouseCoopers

[3] Securities Industry Association Compliance Report, 2006

[4] META Group research conducted on behalf of PricewaterhouseCoopers

[5] Holland & Knight, 2006

[6] Many companies also consider adherence to internal policies within the scope of "compliance."

OpenPages

201 Jones Road, Waltham, MA 02451
Tel: 781.647.3800 Fax: 781.647.4300
Web: www.openpages.com