protiviti®
Risk & Business Consulting.
Internal Audit.

The Bulletin

Volume 4, Issue 10

Is Your Compliance Management Making a Difference?

Compliance management consists of the organization's policies and processes for adhering to applicable laws and regulations. It requires metrics, measures and monitoring that provide assurance to management and the board that established policies and procedures for fostering compliance and responsible business behavior are performing as intended. Without effective management of the compliance risks that really matter, the organization is reactive, at best, and noncompliant, at worst. This issue of *The Bulletin* focuses on the issues around compliance management, its current state, true cost and value proposition, as well as its organizational structure and ways it can be improved.

The Present State of Compliance

For many companies, complex accountabilities for compliance have evolved in an ad hoc manner over a long time. Often, internal and external pressures result in changes being implemented at such a pace that the new policies, procedures and controls are added onto the existing management structure with little or no rationalization of how they interact within the existing compliance framework and business processes. As these new policies, laws and regulations have evolved, several elements of compliance management common to many companies have emerged. These elements include fragmented control environments, unnecessary and often redundant infrastructures, lack of automation, duplicative requests of process and risk owners, reduced organizational transparency, inefficient communications and high audit costs.

Take, for example, a global financial services firm that determined the need to align its nonfinancial risk management and control functions in order to transition its organization toward a single, integrated approach for risk assessment, issues management and reporting of nonfinancial risks and controls. At this institution, 10 different subfunctions had their own risk assessment and management within five functional silos at the corporate level, resulting in separate responsibilities, processes, frameworks and platforms. A common control framework did not exist, and the compliance and audit oversight functions utilized a variety of inefficient and redundant tools and systems to support their respective activities. While audit costs continued to increase over time, management was concerned that the number of compliance incidents and exceptions remained as high as ever. Therefore, the firm's business motivation for streamlining compliance was to identify significant cost reductions by eliminating duplications and instituting the sharing of knowledge without compromising the effectiveness of the compliance effort.

This is just one example. What we're observing is an ongoing spiral of change resulting in the following challenges for many companies in different industries that create similar opportunities for improvements:

- **Absence of a seat at the decision-making table,** resulting in failure to give adequate recognition of compliance considerations in making business decisions, reduced emphasis on compliance in favor of achieving short-term business objectives, and an unclear focus with respect to articulating important control matters
- **Proliferation of operating silos,** which drive myriad risk and control activities feeding a high-cost internal control structure and overlapping resource demands in large organizations (such as multiple self-assessment programs)
- **Gaps and overlaps in ownership of control responsibilities,** which drive missing and duplicative internal controls and assurance activities
- **Fragmented, diffused reporting of risk and control data,** which leads to a lack of transparency and uninformed decision-making about the control structure
- **Mismatches with stakeholder expectations,** as some process owners perceive that the new activities put a drag on operational efficiency, resulting in failure to embed the activities in day-to-day business processes

Accepting the above challenges as mere status quo comes with a cost, as it ultimately contributes to an ineffective and inefficient control structure. The lack of transparency into what really matters in a distributed compliance function in which everyone is responsible for compliance makes it difficult to fully understand the end-to-end compliance infrastructure, including where it has been overbuilt, where redundant

investments have been made, where controls may be ineffective or nonexistent, or where large compliance risk exposures exist that are neither identified nor understood.

In what position does this state of affairs leave the board of directors and executive management? Only when a fiasco occurs (e.g., regulatory penalties and fines for noncompliance, a major controls breakdown or some other debacle that tarnishes the organization's reputation and image in a manner that is visible to the public), do the board and management begin to realize that a proactive approach to reducing reputational risk might be worth considering. Until then, most organizations are in the same position of "hoping and praying" that "what happened to other companies isn't going to happen to us" – knowing full well that, if the unexpected does happen, the organization will be thrown immediately into crisis management mode and damage control will become the order of the day.

The True Cost of Compliance

Lack of transparency into compliance and the reality that it often only becomes a top-of-mind issue in times of crisis suggest that it is very difficult to engage senior management and the board in addressing the question of how compliance can be proactively managed in a cost-effective way.

Undertaking a quality focus on managing compliance with the same passion with which management often attacks the improvement of core operating processes can both reduce costs in specific areas and increase confidence that risks and compliance are effectively managed. We ask two questions:

- Is it time for management to take a fresh top-down look at the design of the organization's compliance management infrastructure and ensure that it is focused on the right compliance areas and operating in a cost-effective manner?
- Does management know what the true cost of compliance is and, if so, has the cost of administering compliance processes become expensive enough to warrant closer attention?

Compliance is a real cost that each organization is incurring – right now – every day. It is reasonable to expect these costs to rise as the complexity of business processes and risks increases and global, regional and local regulations proliferate. For many companies, the rate of increase in compliance costs is an unknown because they haven't quantified their spend. The true cost of compliance consists of three elements:

1. The cost of internal compliance efforts, both specifically identifiable in various functions and embedded within processes (including specific process activities, internal controls, supporting technology, metrics, monitoring, audits and reporting)
2. The cost of oversight at the board and senior, functional unit and middle management levels
3. The cost of noncompliance (e.g., fines, penalties, lost revenues and loss of brand equity, among other things)

Ten Warning Signs Evidencing a Reactionary Approach to Compliance

1. Board members, senior management, process owners and compliance managers have different views as to the strength of the organization's compliance culture and nature of its compliance risk appetite.
2. A lack of transparency as to who is responsible for the most critical compliance tasks.
3. A "silo mentality" to risk management and compliance, which leads to a high-cost structure, overlapping self-assessments, and other demands of process and risk owners.
4. Improvement projects rarely result in sustainable change in the processes of the business.
5. Risk and control reports overwhelm recipients with data and provide very little insight.
6. No one knows how much the compliance spend is.
7. Periodic compliance risk assessments rarely impact business plans and decision-making.
8. A fragmented control structure and lack of automation leave management without an entity-level capability to oversee what really matters.
9. The same compliance issues resurface time after time for review and investigation.
10. No one can describe a holistic view of the end-to-end compliance infrastructure.

Quantification of spend is a whole discussion in and of itself. Start with the budgetary process, identifying the departments with a primary compliance focus. Estimate compliance FTEs and other costs embedded within established business processes. Recognize that there may be some overlaps with risk management. The quantification approach can also get as granular as tagging specific controls and events as compliance-related in GRC platforms and adding compliance cost categories to procurement and IT tracking mechanisms.

With the above as a context, the benefits of compliance investments become clearer. They include the reduction of risk of noncompliance to an acceptable level, as well as sustaining reputation and enterprise value. The focus is not necessarily on reducing compliance spend, but on maximizing effectiveness of that spend.

THE VALUE PROPOSITION OF COMPLIANCE

Managing compliance in a proactive, holistic manner can result in lower costs and increased effectiveness by reducing complexity and redundancy and making entity-level processes

more efficient and effective in providing the necessary oversight. Clearer articulation of objectives, roles, responsibilities and accountabilities lead to more effective risk and compliance processes. Simply stated, everyone knows his or her responsibility. Improved transparency into compliance performance through effective metrics, measures and monitoring leads to more effective risk-based decision-making and increased ability to anticipate issues and reduce reaction time when surprises occur. Other benefits include more meaningful compliance assessments and increased efficiency through effective coordination of the activities of internal audit, operational risk, risk management oversight and compliance, as well as a single system of control to provide compliance with laws, regulations and internal policies that is flexible enough to accommodate inevitable changes in the business environment. All of these value points increase cost-effectiveness and help reduce the growth of compliance-related spend.

The Chief Compliance and Ethics Officer (CCEO)

A company's CCEO is primarily responsible for overseeing compliance within an organization, ensuring that the company and its employees are complying with applicable laws and regulations and with internal policies. Typically reporting directly to the chief executive officer (CEO) or another C-level executive (e.g., chief administrative officer, chief operating officer, chief legal officer or general counsel, etc.) with dotted-line reporting to the board or a subcommittee of the board (e.g., the audit committee), the CCEO position has traditionally existed at companies operating in heavily regulated industries. Over the years, however, more companies and institutions have appointed a CCEO to play a lead role in understanding and coordinating the organization's fragmented compliance efforts and reporting on the state of compliance.

In the context of the current state of compliance, a CCEO should establish standards and implement procedures to ensure that compliance programs throughout the organization are cost-effective in preventing, deterring, detecting and correcting noncompliance with applicable rules and regulations. In this capacity, he or she periodically reports to executive management and the board on whether the compliance policies and procedures in place are effective and efficient in operation. In addition, he or she should inform management and the board periodically about important issues, challenges to compliance and material violations, and provide insights and guidance on appropriate steps to take to address those issues and updates on the progress of implementation of any compliance improvement initiatives.

To discharge these responsibilities, the CCEO must, among other things:

- Maintain current knowledge of laws and regulations, including changes over time, and conduct an annual enterprisewide compliance risk assessment to prioritize the organization's most significant compliance risks.
- Develop and execute a cost-effective plan for monitoring the top compliance risks and overseeing implementation of the compliance program, including development of whistleblower policies and programs that meet legal and regulatory requirements.
- Maintain a current ethics policy and have the budget and resources to ensure it is communicated, monitored and reinforced.[1]
- Develop and oversee distribution of education, training and resource materials focusing on critical elements of the compliance program.
- Coordinate internal compliance reviews and monitoring activities, including periodic reviews of specific units and functions, to ensure compliance programs are working as expected.
- In cooperation with the chief legal officer and executive management, interact with regulators, respond to government investigations and inquiries, and conduct independent investigations in response to reports of problems, external reviews, "hotline" calls or suspected violations.
- Ensure compliance programs are updated periodically in light of changes in the needs of the organization and revisions in applicable laws and regulations.

The CCEO has a tough job. The focus on complying with new regulations, preventing compliance and ethics violations, and remediating compliance and ethics violations can be very demanding, particularly in large and complex companies. To be truly effective, the CCEO must be supported by the CEO, senior executive team and the board of directors. In this context, "support" means a number of things. First, it means the CCEO's role is clearly defined. Second, it means that the CCEO has sufficient resources in both people and tools. Third, it means that his or her role is supported at all levels of the organization, as compliance is everyone's responsibility. Finally, it means that he or she has the appropriate access to the top when circumstances require timely escalation of issues. In summary, the CCEO must have the seniority, authority and means to act when necessary.

Organizing Compliance

Following are several elements of an effective compliance program for executive management and boards to consider:

- **Board oversight:** Proactive understanding of potentially significant compliance risks and oversight of the relevant compliance program by the board or one of its standing committees help to establish an effective "tone at the top."
- **Executive management supervision:** Coordination and management of the compliance program by a designated senior executive (e.g., the CCEO) is vital for organizations with complex, diverse operations.
- **Policies, standards, procedures and reporting mechanisms:** Documented and up-to-date compliance policies

[1] In some companies, responsibilities for managing compliance and ethics are assigned to different individuals.

Some Questions to Consider When Evaluating a Compliance Management Structure

While there is no one-size-fits-all approach, there are several design principles relating to the compliance roles and authorities at various levels of the organization. These are expressed in the questions below:

- What are the roles of the board and the CEO? Effective compliance management starts at the top.
- Does the executive committee have time to focus on compliance issues, or is it necessary to designate a separate subcommittee? If there is a management compliance committee:
  - Who is on it?
  - What are its roles and responsibilities?
  - How does it interface with the operating and functional units, as well as with the board?
  - Does it have a charter?
- Does the organization designate a CCEO or equivalent executive to assume overall responsibilities for compliance management? If yes:
  - Is he/she independent of the core business activities?
  - To whom does he/she report (e.g., to the CEO, another C-level executive and/or to the board of directors, or a standing committee of the board)?
  - What are his/her overall roles and responsibilities, as summarized in the job description?
  - Is his/her role consultative (assess and recommend) or authoritative (approve) or both?
  - Is there adequate support staff to enable the executive to carry out his/her responsibilities?
- What are the roles and responsibilities of business unit, divisional and functional management as they relate to compliance? In particular, what will be the relationship or division of responsibilities among compliance, legal, risk management and internal audit?
- To what extent should the compliance function be centralized (i.e., all personnel with compliance responsibilities report to the CCEO rather than through their respective lines of business)?
- Do governance functions with an influence on compliance (e.g., internal audit, EH&S, value at risk review, etc.) periodically report on compliance matters?
- Are there unique compliance risks inherent in the organization's business model requiring special attention (e.g., environmental issues, health and safety, Basel II and corruption risk)?
- Regarding the priority compliance risks:
  - Is there an enterprisewide view as to what they are?
  - Is there a risk owner assigned to manage each risk?
  - Are there gaps (no risk owner) to be filled?
  - Are there overlaps (too many risk owners) to be eliminated?
  - Are compensation practices incenting the desired behaviors?

Depending on the answers to these questions, an appropriate compliance oversight structure should be designed with an emphasis on keeping it as simple as possible.

and standards in critical areas, along with communication of this information to employees across the organization, are two of the most important elements of an effective compliance program. In addition, an affirmation procedure requiring that critical employees, vendors and contractors provide written statements that they are in compliance with specific laws and regulations may be useful. Effective mechanisms for individuals to report criminal conduct, concerns and other complaints involving potential compliance violations may be appropriate as well.

- **Risk assessment and due diligence activities:** The risk identification process should include explicit consideration of compliance risks. In addition, appropriate subject-matter experts should be accountable for monitoring changes to the regulatory environment continuously and identifying the process modifications required in the compliance areas for which they are responsible. The organization should exercise appropriate due diligence with respect to new employees, joint venture partners and third-party agents to ensure they have the necessary background, resources and experience to discharge their responsibilities. Appropriate compliance language and representations should be incorporated in third-party contracts.
- **Effective internal controls and monitoring:** Many compliance areas have reputational impact. Effective internal control over financial reporting is critical. So are controls over environmental, health and safety issues, security and privacy matters, FDA compliance, anti-money laundering and other compliance domains, depending on the industry. Due to compliance being managed in silos by different groups (e.g., the CFO organization, human resources, etc.), it is important that gaps and overlaps be avoided. Periodic audits of compliance program policies, procedures and controls to assess their effectiveness at ensuring compliance at all levels and across the organization provide welcome assurance to executive management

and the board. Areas of noncompliance and recommended enhancements to the organization's compliance in specific areas (e.g., corruption risk, HR policies, health and safety, etc.) should be reported to senior management and to the board on a timely basis.

- **Training and awareness programs:** Compliance awareness education and training for employees, third-party agents and consultants conducting business on behalf of the organization out of the home country are necessary to ensure that everyone is knowledgeable about the appropriate behavior and legal requirements.
- **Investigatory and disciplinary mechanisms:** Thorough investigation and remediation of reported potential compliance violations are vital to establish the necessary discipline. Disciplinary mechanisms that are consistently enforced for those who violate the compliance policy send an important message.

Companies have a due diligence obligation to establish policies and procedures that provide reasonable assurance that the organization is adhering to the requirements of applicable laws and regulations and internal policies. While not intended as a one-size-fits-all approach, the above elements provide evidence of such due care and can help lay a foundation for an effective compliance program. In this regard, particularly in highly regulated industries, compliance risk managers need a seat at the proverbial table to ensure that their advice on compliance matters will be carefully considered. In addition, a framework may be useful to the CCEO or other executives in scoping out the focus and domains of the compliance management process.[2]

Streamlining Compliance

Because adjustments to the internal control structure have been case-by-case and bottom-up in terms of their evolution over a long period, there have been few, if any, top-down efforts to periodically assess whether the resulting infrastructure makes sense from an organizational design standpoint and is sufficiently transparent and understandable. As a result, many large organizations have substantive untapped opportunities for improving efficiencies in compliance management.

Quantifying the current cost of compliance provides a starting point for undertaking steps to make compliance more cost-effective. Once management quantifies compliance spend and understands where costs are being incurred and why, redundancies and omissions in the responsibilities and execution of corporate functional activities for compliance can be identified, and areas where more efficient and effective controls are needed can be rationalized. The objective is to maximize the value of the organization's compliance investment.

[2] One example of a framework is the Red Book 2.0 GRC Capability Model, published by Open Compliance and Ethics Group, which includes many aspects of a compliance management process.

Compliance Management in Higher Education

In higher education, an effective compliance program should span all of the institution's departments and functions and be supported by the right resources, technology and other tools. The institution should establish clear compliance objectives supported by leadership and the board of trustees, and include the participation and "buy in" of business process owners who are responsible for managing compliance risks on a day-to-day basis. For example, the following objectives provide a blueprint for establishing and maintaining compliance programs:

- Create the appropriate tone at the top by establishing a climate that supports discussing compliance issues openly and with integrity, even if doing so may create short-term exposure for the institution.
- Embed compliance in the institution's culture so it is part of every person's job and all stakeholders support the concept.
- Establish clear ownership and accountability for compliance activities performed across the institution and related decision-making, including ensuring actions are consistent with words.
- Establish an efficient compliance management framework, including a protocol to identify and address new or changing requirements.
- Strike an appropriate balance between fulfilling the institution's mission and compliance risk management objectives.
- Proactively monitor compliance, minimizing the need for inefficient, reactive "fire-fighting" exercises to close gaps.
- Reduce the risk of reputational damage and monetary and other penalties caused by compliance issues to an acceptable level.

The above objectives provide principles for designing compliance management programs in higher education institutions. To illustrate, a distinguished private university sought to redesign its compliance function in response to several high-profile compliance failures. The current function was assessed using benchmarking information on similar universities. Using the above design principles, management and the board collaborated to design a compliance structure and function that could identify and prevent compliance risks proactively by providing the proper reporting channels and tools to identify and address compliance risks.

Returning to the global financial services firm we referred to earlier, five general design principles were used by the organization during its project to streamline compliance:

- **Balanced operating model** – Strive for lean central functions and empower the regions, with central functions focusing on global initiatives, policy and strategy development, oversight, and consolidated reporting. Stay within the boundaries of established regulatory requirements for oversight, business accountability and independence. Take into account the activities of independent functions such as internal audit and value at risk compliance to facilitate oversight.
- **Basic governance principles of internal control** – Adopt an operating philosophy of "defense in depth" with multiple "lines of defense" to push responsibility for compliance and related internal controls down to the lowest level possible, unless it is not economically feasible to do so:
  - **First line of defense:** The heads of business who are primarily responsible for managing compliance risks in their respective units and pushing down responsibility to the appropriate process and risk owners.
  - **Next line of defense:** Risk and control functions that are independent from the business units and coordinate, oversee and challenge compliance responses, act as advisors and have power to escalate or veto high-risk activity in the first line.
  - **Final line of defense:** Internal audit provides an independent assessment of the design and effectiveness of internal controls of the first- and second-line activities.

  Expectations were set for each line of defense to perform "first-time right" with respect to its responsibilities and, where feasible and appropriate, rely on the activities of lower lines.
- **Holistic enterprisewide approach** – Establish a consistent top-down, organizationwide view of all compliance risks to ensure complete coverage of risks at all levels in the firm. Incorporate these risk assessments and related risk information into decision-making processes.
- **Prudent cost reduction emphasis** – Establish overall efficiency and control objectives with a purpose of rationalizing a more efficient design of controls and driving a more focused internal control structure. Perform risk assessments and controls testing once and reuse the results rather than engage in redundant efforts. Adopt cost-efficient systems and infrastructure across all risk and control functions, with a bias toward leveraging existing systems rather than planning new systems.
- **"Quick win" scenarios focus** – Define these scenarios as initiatives for which management could realistically expect quantitative and qualitative benefits to materialize within six to 12 months.

With these five design principles driving the project, a more streamlined, end-to-end view of risk management and compliance resulted in the following outcomes:

- Improved coordination across the organization of control requirements-setting, alignment of management and control activities, and streamlining and integration of reporting around compliance and other risks
- More clearly articulated objectives, roles, responsibilities and accountabilities leading to more effective rationalization of risk management, compliance and internal control policies and procedures
- Reduced complexity and redundancy and increased efficiency and effectiveness of entity-level oversight processes
- Improvement in the quality, sustainability and cost-effectiveness of the internal control structure
- Improved transparency into performance of risk management and compliance activities through more effective metrics, measures and monitoring

While executive management's support for the initiative evidenced an effective tone at the top, the improved articulation of requirements for the control environment, better coordination of control requirements-setting and more effective alignment and integration of risk management and compliance activities to drive better reporting, managing and controlling of risks and compliance resulted in a stronger "tone in the middle."

Summary

Companies should ensure that they are implementing a holistic, top-down and proactive approach to overseeing risk management and compliance. A fragmented control environment, unnecessary infrastructure, excessive manual controls, redundant requests of process owners, high audit costs and other symptoms of a reactive compliance infrastructure should be re-examined. Undertaking a quality focus on managing compliance with the same fervor with which management often attacks the improvement of core operating processes would both reduce costs significantly (by as much as 30 percent or more in specific areas) and lead to better management of risks and compliance.

protiviti®
Risk & Business Consulting.
Internal Audit.