



THE
COMPLIANCE
AUTHORITY



GRC Industry Survey 2008: A Benchmark For Compliance Programs and Spending

Chrisan Herrod, Executive Editor, The Compliance Authority
Sanjay Anand, Chairperson, SOX Institute

Executive Summary

Over the past decade, the landscape of regulatory compliance and industry standardization has become increasingly complex. Companies at every point in the spectrum – from SMBs to large enterprises to multinational corporations – have been deeply impacted by regulations like the Sarbanes-Oxley Act (SOX Act) and the Health Insurance Portability and Accountability Act (HIPAA), as well as standards like the Payment Card Industry Data Security Standard (PCI DSS).

This survey, conducted in early 2008 by The Compliance Authority and The SOX Institute, sought to assess perceptions of compliance, spending related to compliance programs, and approaches to mitigating compliance costs. The survey reached a broad spectrum of participants, with 455 respondents from a representative range of companies and occupations within the compliance industry. A full 20% of the respondents were from the executive suite.

The largest category of respondents came from Compliance (39%), followed by Internal Audit (22%), IT (20%), and Finance (11%). Over 57% came from companies with more than 1,000 employees and a full 24% came from companies with more than 10,000 employees. Approximately one-third of respondents were from the Financial Services sector, and two-thirds from a broad range of industries.

The majority of respondents indicated that compliance was an ongoing process, and that SOX Act compliance was a top priority. Only 15% of respondents stated that compliance costs were declining and a full 40% reported increases in compliance spending.

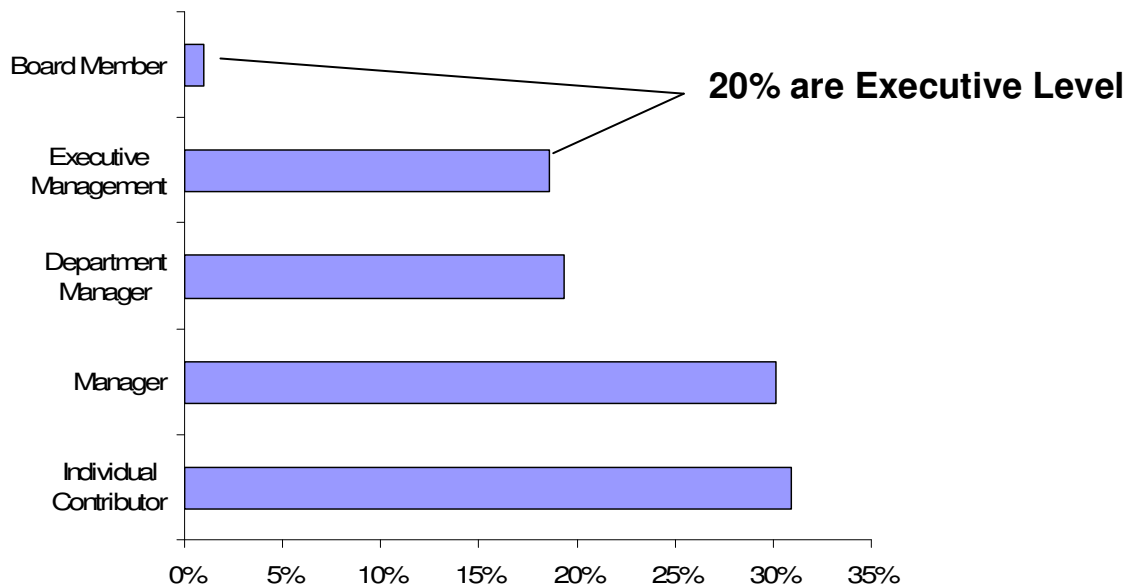
The most popular methods of reducing compliance costs involved standardization of processes and staff training. Yet the survey revealed that a full 57% of respondents could further reduce costs by sending their staff to training. Two of the leading barriers to successful compliance programs, organizational impediments and compliance staffing, can both be addressed by comprehensive training programs.

A significant number of respondents (22%) expressed concern that their organization's risk of noncompliance was increasing. While 88% of respondents acknowledged the importance of eliminating barriers to successful compliance programs, only 57% used tools to automate a portion of their compliance activities. Likewise, only 50% of respondents expressed satisfaction with their current tools.

Organizations cite two primary factors when evaluating software solutions: the ability to manage risk and ensure process integrity.

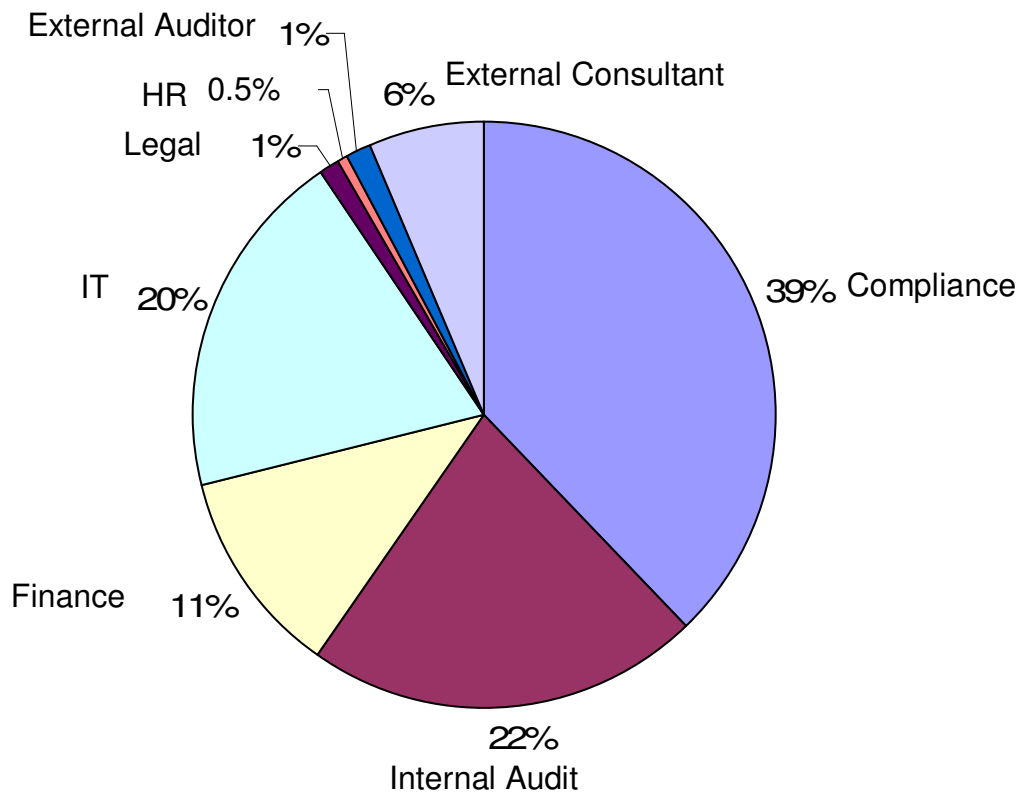
How would you characterize your role within your organization?

Over 70% of respondents have managerial or higher authority within their organizations, with a full 20% coming from the executive suite. The participation of senior executives and mid-level management are not surprising, given the fact that CEOs and CFOs are responsible, particularly under the SOX Act, for compliance initiatives. It is important to note that individual contributors play an integral role in compliance, and can often determine whether a compliance program succeeds or fails.



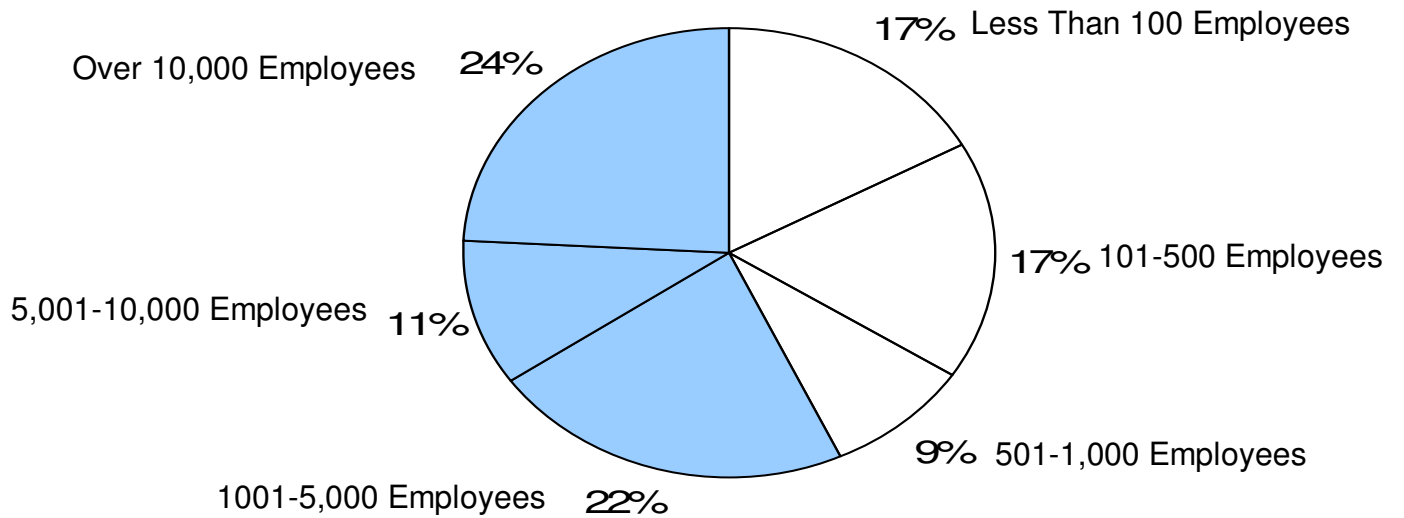
What is your primary responsibility within the organization?

All of the major areas of compliance are represented. The fact that only 39% cited compliance as their primary responsibility indicates that, in many organizations, the burden of compliance activities cross departmental boundaries and reach every corner of the organization.



How large is your organization?

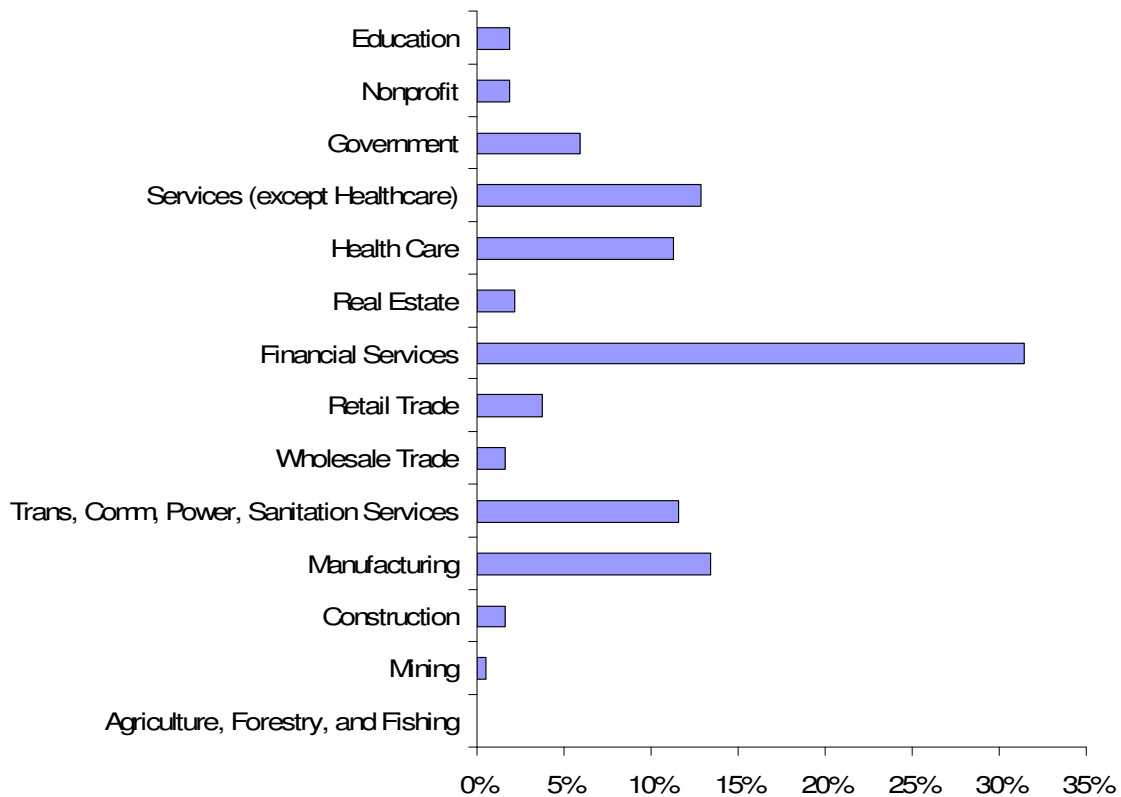
While the majority of respondents are from larger organizations, the split is relatively even. Compliance issues clearly touch organizations of all sizes, a trend that is expected to increase.



What is your primary industry?

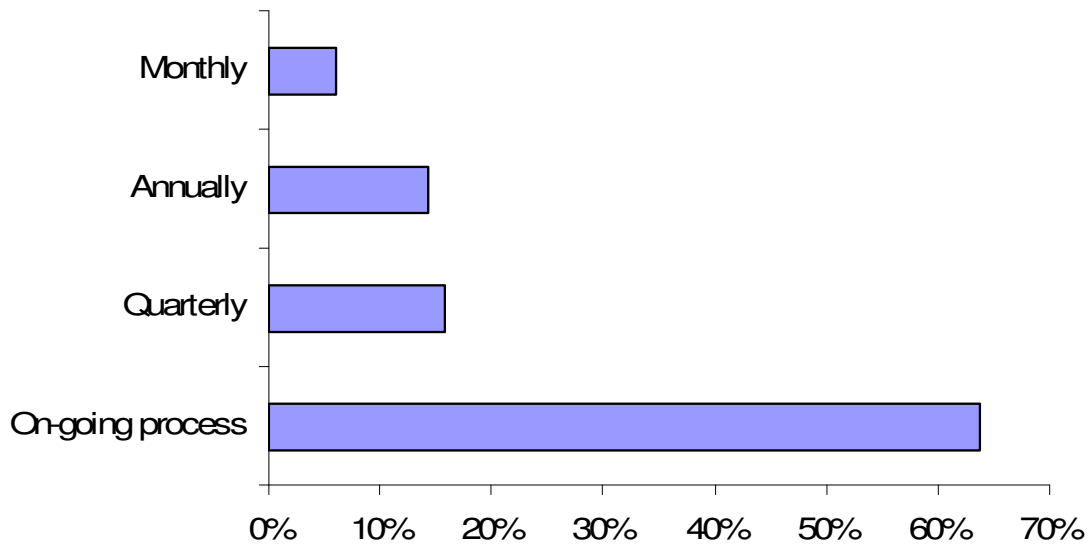
There is broad industry representation, with a preponderance of Financial Services firms and an underrepresentation of some sectors. There is a solid representation of Health Care, Manufacturing, and Transportation, Communication, Power, and Sanitation Services firms.

The disproportionate representation of the Financial Services sector is likely due to two factors. First, Financial Services and Health Care have historically faced the most regulation. Second, with the recent increased scrutiny of the Financial Services industry, these organizations are under a great deal of pressure to ensure that they have effective compliance programs. Despite this weighting, the survey still reflects the views of a broad range of industries.



How often does your organization perform compliance audits and associated reports?

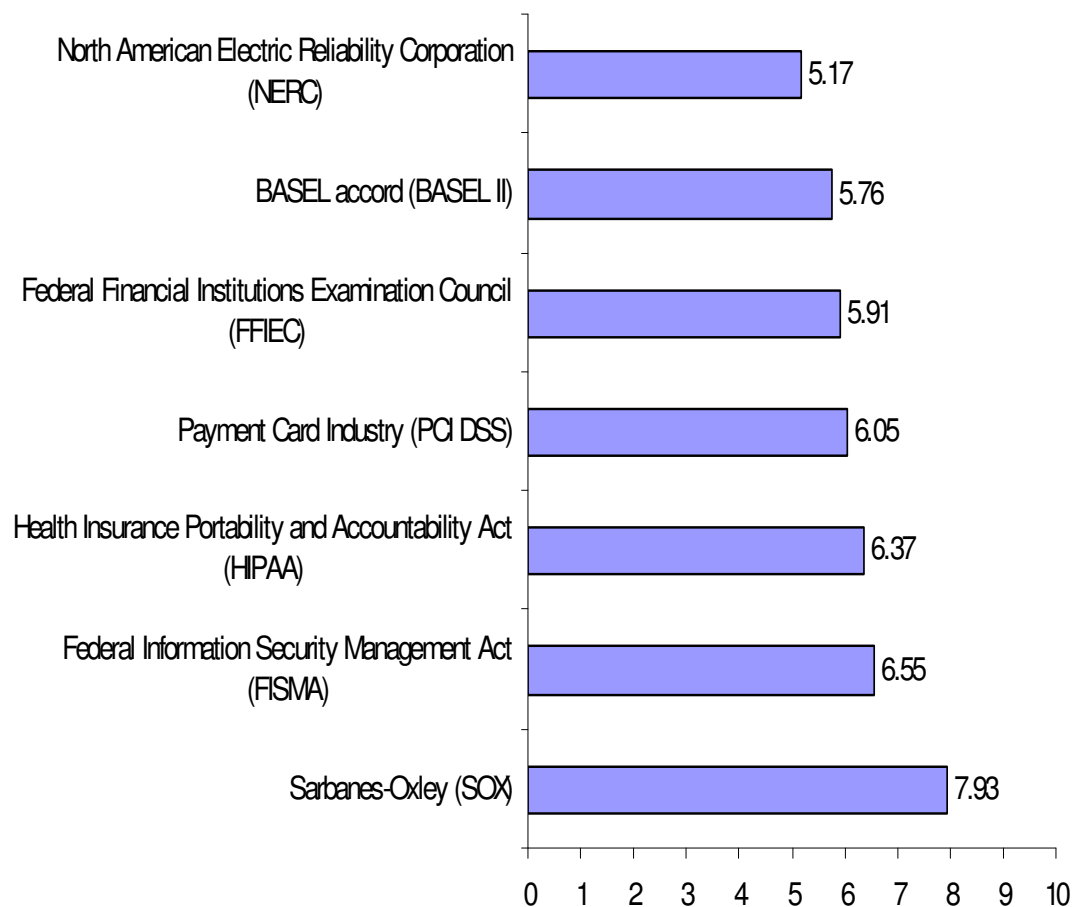
Over 60% of respondents reported that compliance-related activities are performed on an ongoing basis. This frequency, combined with the fact that compliance is but one of the duties respondents have, indicates a significant need for standardization and automation of tasks. As companies adopt GRC methods, compliance is ceasing to exist as a separate responsibility, and is instead becoming more integrated in all processes. Over time, this is raising the bar for all organizations, as external auditors are beginning to expect this level of sophistication.



Please rank the following regulations with respect to your organization's compliance priorities.

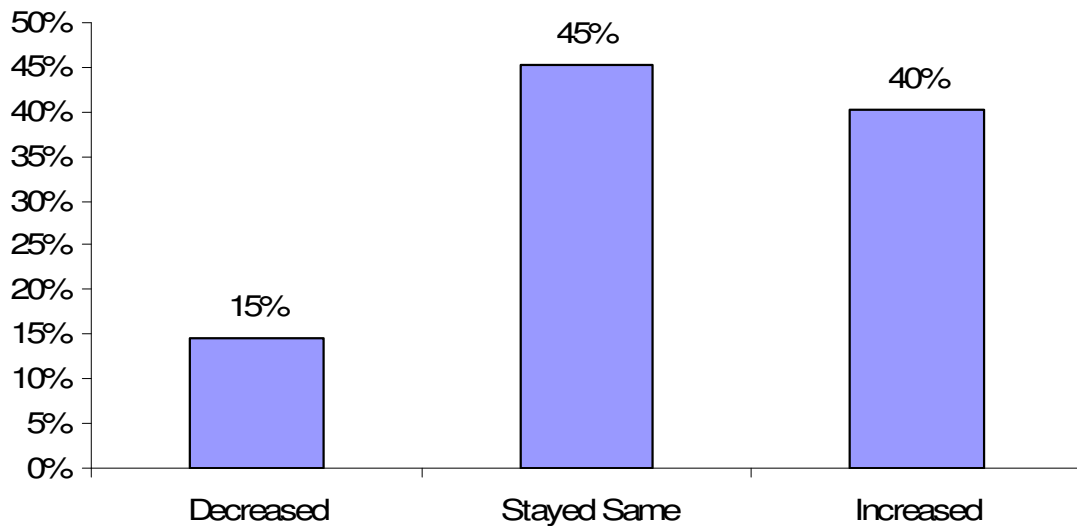
For most companies, the SOX Act remains their most important compliance priority. This may be due in part to the survey's sponsors' reach into the market, which has largely been driven by the SOX Act. However, other regulations, specifically the payment card initiative PCI DSS, have a broad reach, as any organization that accepts credit cards must comply with this standard.

Complying with PCI DSS has largely been IT-driven. Many people in organizations are unaware of this initiative, which is indicative of an improvement in organizations' ability to meet standards and regulations. In the aftermath of the SOX Act, it appears that organizations are more easily able to adapt to and comply with new standards and regulations. This may be an indicator that the framework for SOX-related controls and procedures can be repurposed for other forms of compliance, thus lowering implementation costs.



How has your organization's spending on compliance changed in the last year?

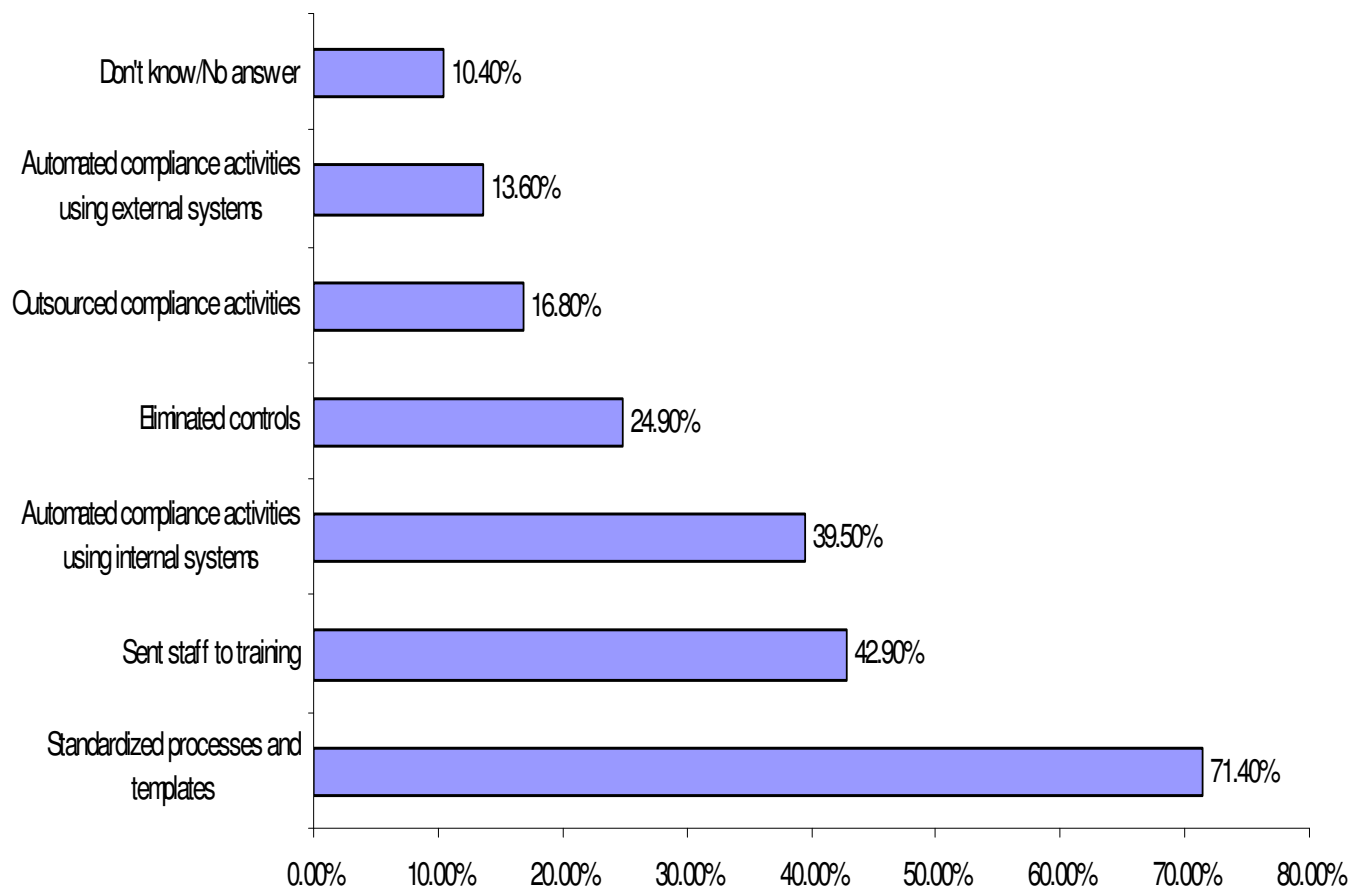
Forty-five percent of respondents reported that compliance costs remained steady over the past year, while a full 40% indicated that spending had increased. Sustained or increased spending can be attributed to three factors. First, SOX Act compliance has moved beyond only accelerated (large cap) filers, and now encompasses every publicly traded company. Based on data from accelerated filers, it appears as though first-year and second-year compliance costs are significantly higher than those in subsequent years. Second, an increased number of regulations and standards drive compliance costs higher. Finally, companies are investing in automation with the goal of reducing costs long-term, but initial technology-related spending drives up costs for many companies.



Which of the following actions has your company taken to reduce compliance costs?

A surprising number of respondents, 10.4%, reported that they did not know an action that their company had taken to reduce compliance costs. Ultimately, compliance must be integrated into the framework of how a company does business, which is reflected in the standardization of processes and templates, as reported by 71.4% of respondents. If compliance is treated as a new and separate project for each reporting period, then expenses remain high. Tangible cost reductions are realized only upon ongoing, standardized procedures.

Close to 43% of respondents reported that their companies used staff training as a mechanism for lowering compliance costs, while close to 40% automated compliance activities using internal systems. Training is critical in providing employees with the knowledge and awareness they need to plan and execute a compliance program. Technology can reduce costs, but ultimately it is only as effective as the people who develop and operate it. Compliance requires a top-down flow of information; training plays an important role in that flow of information. Previous research has indicated that companies can realize significant returns on investment from their training initiatives.

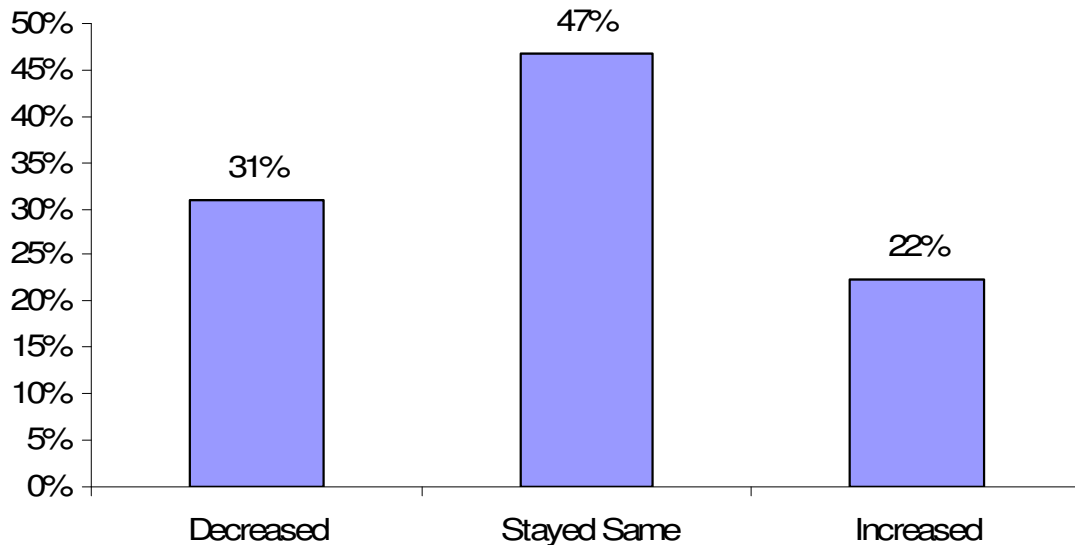


How has your organization's risk of non-compliance changed in the last year?

Twenty-two percent of respondents reported an increased risk of non-compliance in their organizations. This is likely due to two factors. First, as organizations have become more sophisticated in their compliance efforts, regulators and external auditors have begun holding companies to a higher standard.

Second, the penalties of noncompliance have become more far-reaching. In addition to fines imposed by regulators, companies face the prospect of decreased stock value when they are unable to meet compliance objectives.

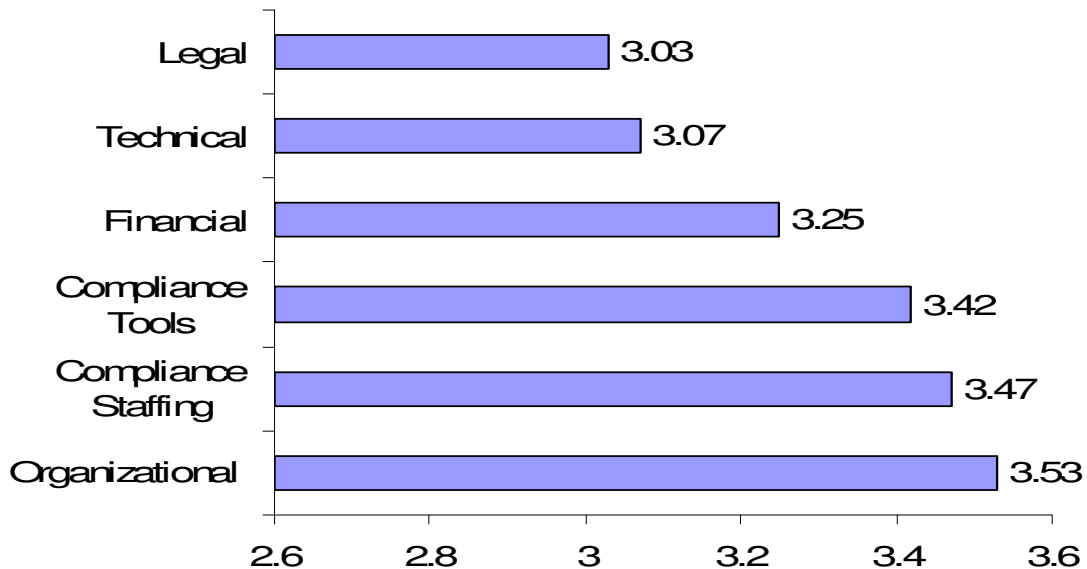
Companies that are seeing a decline in their risk of noncompliance generally have adopted GRC principles and integrated compliance activities into the framework of doing business.



Please indicate the barriers to implementing a successful compliance process

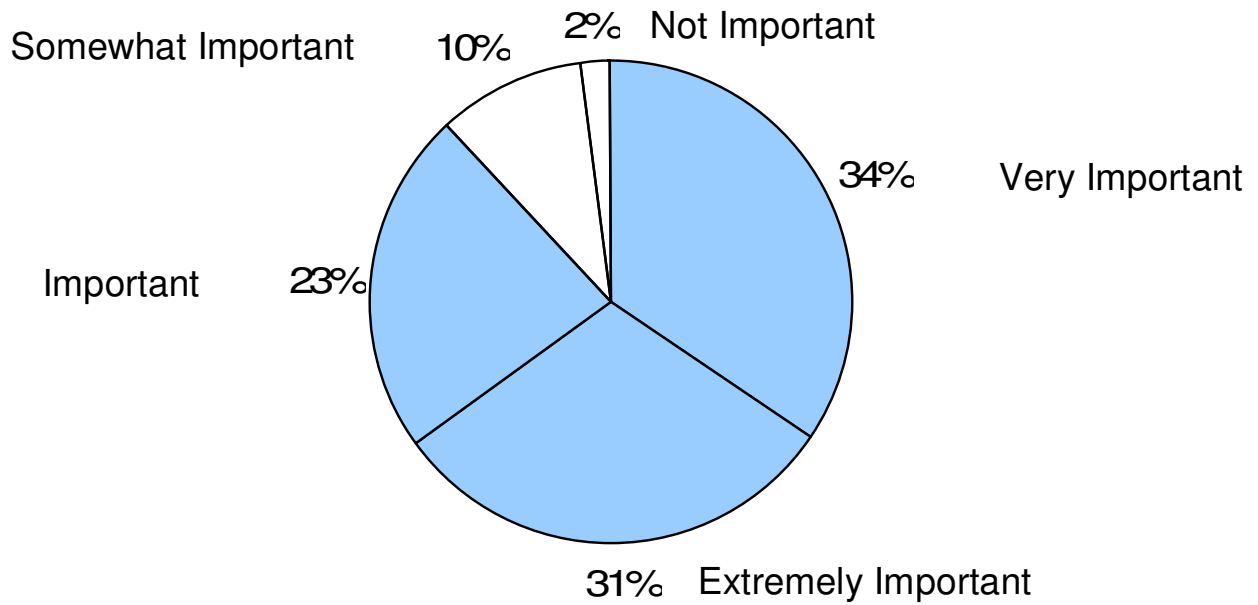
Training can address the two most important barriers to compliance by equipping staff with skills in both change management and the disciplines of compliance. Ultimately, successful compliance programs come from having knowledgeable people who are able to execute the initiative. This was a key frustration for executives in the early days of SOX.

Addressing this frustration was the foundation of The SOX Institute’s certification program. Recruiting knowledgeable compliance professionals remains one of the key frustrations in the marketplace. A significant change that has taken place over the last five years is that there is an increasing variety of resources that professionals can access to gain the knowledge they need to effectively ensure compliance within their organizations.



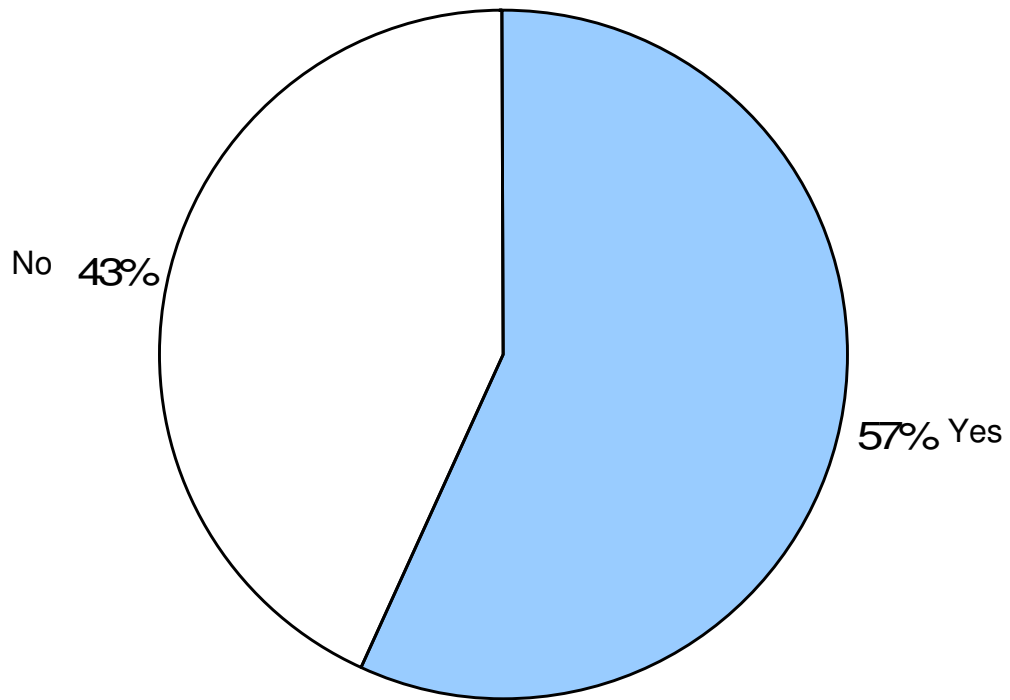
How important is it to your organization to eliminate the barriers to a successful compliance program?

A full 88% of respondents felt that eliminating barriers to a successful compliance program was important. The tone from the top must clearly convey the need to meet GRC initiatives.



Do you utilize tools to automate the compliance process?

The majority of companies (57%) are using tools to automate a portion of the compliance process. Likely, these are workflow tools that sit on top of ERP systems. However, specific compliance tools are relatively new and are likely increase in use over the next several years as the tools become more sophisticated.



What are the business drivers for adopting and deploying compliance tools or solutions?

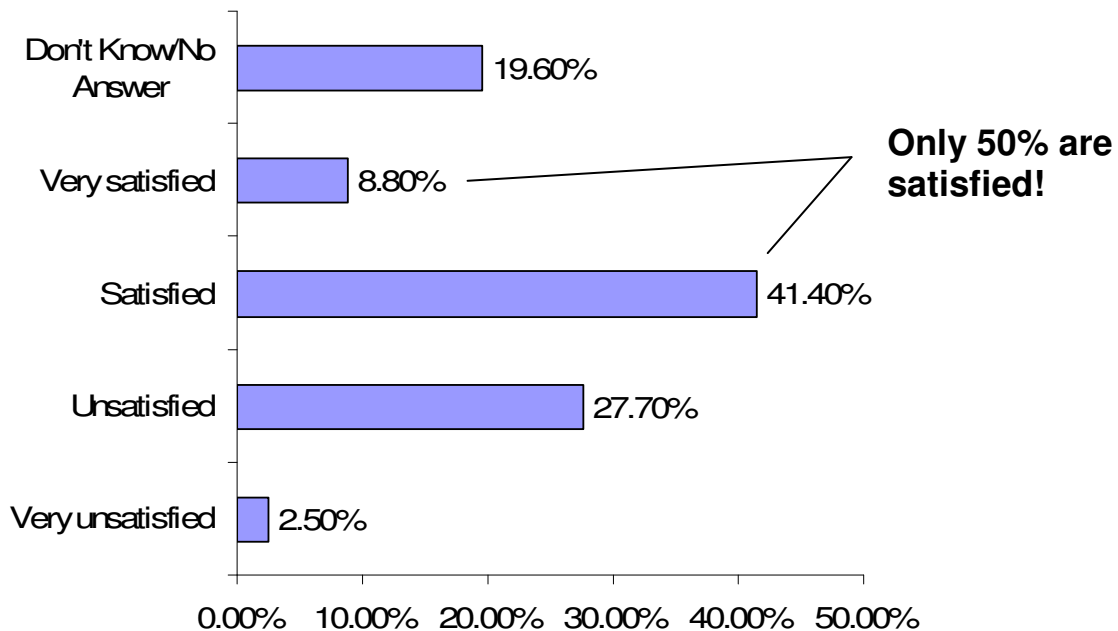
The most significant concerns of compliance professionals are the reduction of risk and the elimination of errors. This is in line with organizations' emphasis on business process re-engineering and enterprise risk management, which are both facilitated through the use of automated tools.



Please indicate how satisfied you are with your existing compliance tools/solutions?

Only half of respondents indicated that they are satisfied with their existing compliance tools and solutions. This is likely because the marketplace is just reaching the level of maturity where the various elements needed to develop effective tools are in place. Companies are also expecting tools to not just automate compliance, but also to improve upon or contribute to business objectives.

GRC will help integrate compliance with business objectives, but a true GRC tool is not likely to be introduced within the next year or two. In the meantime, there are tools on the market to automate aspects of the SOX Act, HIPAA, and other compliance initiatives.



Conclusion

The survey's reach provides an authoritative view of the compliance industry. The survey revealed that the majority of respondents face the same or increasing costs of compliance. For many respondents, the risk of non-compliance is increasing several years after the introduction of the SOX Act.

Training can address many of the barriers that companies face in executing a successful compliance program. There are also unmet needs related to the provision of software tools to address compliance issues. A significant portion of the market is looking for a solution that will satisfy these unmet needs.