Powerful Insights
Proven Delivery.®

Hot Topics in Public Company Transformation

Considering Going Public – Assessing Key Market Trends and Risks Based on Protiviti Research

Throughout the year, Protiviti conducts research and publishes insightful thought leadership on a broad range of issues affecting publicly held companies, ranging from today's top risks to internal audit, SOX compliance, and IT security and privacy. We also regularly address key market developments, such as this year's release by COSO of its new *Internal Control – Integrated Framework*.

These issues should be top-of-mind not only for publicly held organizations, but pre-public companies that are planning an initial public offering. Following is a summary of these studies and insights, along with our viewpoints for pre-IPO organizations. Further guidance on these and other issues is available in Protiviti's *Guide to Public Company Readiness: Frequently Asked Questions (Second Edition)*, which we updated earlier this year with details and commentary about the JOBS Act and other relevant developments for pre-IPO companies.

Top Risks for Companies Today – Executive Perspectives

Rarely has there been a greater need for transparency into the nature and magnitude of risks undertaken in executing an organization's corporate strategy than today. The first question an organization seeks to answer in risk management is, "What are our most critical risks?" The organization's answer lays the foundation for management to respond with appropriate capabilities for managing these risks.

To provide perspectives about the nature of potential risks this year, **Protiviti** and **North Carolina State University's ERM Initiative** surveyed more than 200 business executives to obtain their views about what risks they believe are likely to affect their organizations over the next 12 months. The respondent group, comprised primarily of board members and C-suite executives, provided their perspectives about the potential impact of 20 specific risks.

This survey provides insights across different sizes of companies and across multiple industry groups as to what the key risks are today based on the input of the participating executives. Among the notable findings:

- Executives are significantly concerned about the magnitude and severity of risks that could affect the achievement of profitability or funding goals over the next year.
- Overall, two risks stand out as being of the highest concern:

protiviti®
Risk & Business Consulting.
Internal Audit.

    - Risks related to profitability constraints due to overall economic conditions that will limit growth opportunities; and
    - Concerns about the potential for regulatory changes and heightened regulatory scrutiny that will affect how products and services will be produced and delivered.
- In addition to concerns about the economy and regulatory change, the other risk viewed as having a major impact in the coming year relates to growth opportunities being restricted by uncertainty surrounding political leadership in national and international markets.
- Other top risks include:
    - Succession planning and attracting/retaining top talent
    - Anticipated volatility in global financial markets
    - Cyber threats, privacy, identity management, and other information security and system protection risks

Pre-Public Company Point of View

It is important for pre-IPO organizations to monitor the economic landscape and regulatory environment on a regular basis, as well as other risks germane to their organizations. Often, management will maintain its focus on important challenges such as preparing for the company's initial public offering while ensuring the company's core operations continue and seeking new opportunities for innovation – and rightfully so. Management may identify, assess and manage certain key risks at a particular point in time, but it neglects to monitor the risk landscape on a regular basis. The risks identified in this study are presenting new challenges to organizations around the world, including pre-IPO companies.

Internal Audit

As indicated in the results of Protiviti's 2013 Internal Audit Capabilities and Needs Survey, responding to rapidly changing business processes and establishing more collaborative relationships with colleagues emerge as major themes for today's internal audit functions. Among the key findings from our study:

- **Social media remains a top concern**. Understanding social media applications is a critical priority for internal auditors. This reflects both the rapidly expanding use of social media throughout the enterprise and the risks inherent in social media.
- **Changes from regulatory and rulemaking bodies are garnering attention**. Notable changes including COSO's updated *Internal Control – Integrated Framework* are challenging internal auditors to keep pace with new requirements and resulting changes in auditing practices and processes.
- **The nature of fraud is changing – as are the ways internal auditors address it**. As companies rely more heavily on so-called "big data" to drive decision-making, new forms of fraud are targeting this information. Internal auditors are looking to apply leading-edge techniques as part of their fraud prevention, detection and mitigation activities.
- **There is continued interest in leveraging technology-enabled auditing**. As in previous years of our study, data analysis tools, computer-assisted auditing tools, and continuous auditing and monitoring approaches rank as top priorities for improvement.

- **Internal auditors aim to think more strategically, collaborate more effectively**. The need to enhance strategic thinking capabilities and opportunities reflects the increasing regularity with which internal audit is being called on to share risk-related insight and analysis prior to strategic decisions being made.

Latest developments for NASDAQ- and NYSE-Listed Companies

Recent announcements from the National Association of Securities Dealers (NASDAQ) and New York Stock Exchange (NYSE) are garnering significant attention from companies listed on these exchanges, and particularly from pre-IPO companies planning to be listed on either of them.

In March 2013, the NASDAQ proposed a new rule to require listed companies to have an internal audit function. However, in light of the breadth and nature of the comments that the NASDAQ subsequently received from its issuer community and other stakeholders, it elected in May 2013 to withdraw its proposal so that it may adequately consider these comments.[1] Despite this withdrawal, the NASDAQ has stated its intention to resubmit the proposal, and one possibility is that the exchange will implement the requirement in stages for companies based on their size.

While the NYSE requires all listed companies to have an internal audit function, it just approved a one-year transition period for newly listed companies to establish this function.[2] Under the current NYSE listing standards, a listed company must have an internal audit function to provide management and the audit committee with ongoing assessments of the listed company's risk management processes and system of internal control. Newly listed companies now have one year to comply with the requirement.

Pre-Public Company Point of View

Regardless of the listing exchange selected, it is strongly recommended that pre-IPO organizations set up a risk management program prior to their public offering, either through a formal internal audit function or another approach. The good news is that, in the case of the NYSE, listed companies have some flexibility in how they institute an internal audit function – it may be in-house, co-sourced or outsourced. This flexibility can be highly desirable for smaller organizations that do not have the necessary internal audit expertise. We expect the NASDAQ to offer this same flexibility to listed companies when it resubmits its proposal.

Having a risk management program in place will help pre-IPO companies address key challenges such as those identified in our 2013 Internal Audit Capabilities and Needs Survey, including fraud risk and assuring appropriate controls and procedures for regulatory compliance. Of particular note, internal audit can help ensure there are proper controls within these organizations around social media activities, which often are highly prevalent in a pre-IPO environment – and for good reason.

[1] See Protiviti's Flash Report, "NASDAQ Withdraws Proposed Internal Audit Function Rule with Intent to Resubmit It," May 15, 2013, available at www.protiviti.com.

[2] See Protiviti's Flash Report, "NYSE Approves One-Year Transition Period for Newly Public Companies to Comply with Internal Audit Requirement and Proposes Clarification of Audit Committee Responsibilities," September 16, 2013, available at www.protiviti.com.

IT Security and Privacy: Knowing How – and Where – Your Confidential Data Is Classified and Managed

It's the phone call every CIO fears. It's 3 a.m., and you're notified that there's been a major security breach and data loss at your company. Millions of customer records have been compromised. What's worse, the breach occurred at one of the organization's data management vendors, and there's a realization that 1) you and your company do not know the level of security protocols the vendor has in place, and 2) your company bears full responsibility, under the law and in the court of public opinion.

Fortunately, many CIOs, IT departments, and executive management and information management teams are addressing these issues every day. The results of Protiviti's 2013 IT Security and Privacy Survey indicate a number of positive trends, as well as critical areas for improvement:

- **Information management as a strategic priority** – There is an encouraging rise in the involvement of the CIO in activities including, but not limited to, data governance oversight and execution, along with crisis communications. More CIOs are in place today within companies, reflecting a recognition that data is a critically important asset that must be managed differently and even more effectively than other assets.
- **Lack of key data policies** – One in four companies do not have a written information security policy (WISP) and one in three lack a data encryption policy. These are critical gaps when considering the legal implications of such omissions.
- **Less-than-ideal data retention and storage practices** – The stream of data companies are managing is increasing almost daily, yet few address this volume with a detailed and comprehensive classification system. Many, in fact, treat all of their data the same, rather than classifying it appropriately.
- **Unprepared for a crisis** – In light of the many well-publicized data breach incidents and numerous data breach and privacy laws, a surprisingly high number of companies are not adequately prepared to respond to such a crisis.

Pre-Public Company Point of View

Designing and implementing a scalable IT environment that will meet the needs of a public company ranks among the top priorities for many pre-IPO firms. The most common IT risks they need to address include systems and data related to the accurate and timely production of financial statements; creating, testing, monitoring and managing IT general controls that pertain to SOX compliance; and supporting business process improvements conducted during the readiness effort with related systems and applications changes and updates. In addition, pre-IPO companies, like most other organizations, need to remain very mindful of their security and privacy risks. They must strive to implement appropriate measures and processes that will help ensure the appropriate management of the organization's data and information – otherwise, they open themselves to serious reputation, legal and regulatory risks.

As detailed in Protiviti's *Guide to Public Company Readiness*, numerous IT policies should be assessed and/or established during the readiness effort, and each should be documented.[3] These include policies related to security, data backup, business continuity management and disaster recovery, Internet data transmission, and remote and virtual private network (VPN) access, as well as security and privacy issues related to Internet and data use.

[3] *Guide to Public Company Readiness: Frequently Asked Questions (Second Edition)*, Protiviti, 2013, www.protiviti.com/IPO.

Building Value in Your SOX Compliance Program

As the Sarbanes-Oxley Act (SOX) enters its second decade (and Section 404 nears the end of its first decade), organizations with the most effective and efficient compliance capabilities are learning from the past, rather than repeating it. In fact, despite its relative maturity, SOX continues to pose new challenges for public companies. Recent emerging challenges include:

- Public Company Accounting Oversight Board (PCAOB) inspections of public accounting firms are influencing how external auditors examine the effectiveness of their clients' internal control over financial reporting.
- The updated *Internal Control – Integrated Framework* from COSO requires companies to make refinements to how they assure strong and effective internal controls.

In addition to these regulatory- and standard-driven changes, a disjointed economic recovery along with familiar business disruptions (mergers, acquisitions, restructuring, etc.) also create the need for continuous updates, recalibrations and improvements to existing SOX compliance capabilities.

Key findings from our 2013 Sarbanes-Oxley Compliance Survey reveal that the best compliance efforts remain spry and seek to build value as well as increase effectiveness.

- More companies are adjusting their compliance efforts to focus on high-risk processes and walkthroughs.
- External auditor reliance on these efforts, and on the work of others in general, continues to evolve, due in part to guidance from the PCAOB.
- More companies are shifting SOX compliance oversight responsibilities away from project management offices (PMOs) to internal audit functions.
- SOX compliance costs are rising, as are external audit fees. However, for most organizations the cost of SOX compliance remains at a manageable level.
- Organizations continue to report significant improvements in their internal control structures since SOX Section 404(b) became a requirement.
- The automation of controls remains an enticing option and perhaps the "final frontier" for achieving significant improvements and efficiencies.

COSO Unveils Updated Internal Control – Integrated Framework

In May 2013, COSO – an organization providing thought leadership and guidance on internal control, enterprise risk management and fraud deterrence – announced the formal release of its updated Internal Control – Integrated Framework. The original COSO internal control framework was released nearly 21 years ago. Since then, this time-tested publication has gained broad acceptance and has been widely used, particularly as a suitable – and the predominant – framework in conjunction with reporting on the effectiveness of internal control over financial reporting by public companies listed in the United States in accordance with Section 404 of the Sarbanes-Oxley legislation. Today, this framework continues to be recognized as a leading resource for purposes of providing guidance on the design and evaluation of internal control.

Developed over a two-and-a-half-year period, the new framework and related illustrative documents are intended to help organizations in their efforts to adapt to the increasing complexity and pace of change, to mitigate risks to the achievement of objectives, and to provide reliable information to support sound decision-making. The new framework consists of an executive summary, the new framework itself, several appendices, an applications guide providing illustrative tools, and a compendium of approaches and examples for application to internal control over financial reporting.

For interested parties, the new framework is available on the COSO website (www.coso.org). In addition, Protiviti reviews the updated framework in Volume 5, Issue 3 of *The Bulletin*, as well as in a more-detailed white paper, *The Updated COSO Internal Control Framework: Frequently Asked Questions*.

Pre-Public Company Point of View

SOX, of course, is among the most challenging requirements for newly public organizations. The most significant – but certainly not the only – component of SOX is Section 404(b), which lays out requirements related to internal control over financial reporting (ICFR) that should be in place for a company to achieve compliance with the law. Establishing appropriate ICFR is a challenge that, in our experience, requires four to six quarters of planning and preparation.

Granted, many pre-IPO companies may gain a reprieve from having to comply with certain provisions of SOX Section 404(b) immediately as a result of the JOBS Act and their possible classification as an emerging growth company (EGC). But EGC eligibility is finite (up to five years) and can end immediately if the organization exceeds any of a number of thresholds defined under the law.[4] In addition, newly public companies must still comply with SOX Section 404(a), which requires management to issue an internal control report beginning with the company's second annual report following its public offering, as well as comply with other provisions requiring disclosures and certifications pertaining to the control environment.

As noted above, the predominant framework to assess the effectiveness of ICFR, as well as identify areas of improvement, is the COSO Internal Control Framework, and specifically the just-released New Framework. Gaining a strong understanding of this new framework is another of many priorities for pre-IPO organizations.

The most relevant lessons pre-public companies can glean from recent Sarbanes-Oxley compliance history include the following:[5]

- It is never too early to begin the compliance readiness process, which always requires more time than a compliance team initially estimates.
- A top-down, risk-based approach is critical to a successful and efficient compliance program.
- The number of internal controls is the primary cost driver of Sarbanes-Oxley compliance.
- Because the market for Sarbanes-Oxley compliance talent and expertise remains tight, it is critical to hire resources and/or bring in third-party experts and auditors early.
- A one-size-fits-all approach to compliance does not exist.

[4] Ibid, page 37.

[5] Ibid, page 20.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE 1000® and FORTUNE Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

About Our Public Company Transformation Solutions

Our Public Company Transformation practice (www.protiviti.com/IPO) helps companies assess their level of preparedness for an IPO and assists management with the multitude of private-to-public transformation initiatives. For each client, we help create and execute a plan to optimize the capabilities of its organization, including its internal processes, human resources and information systems, for both a successful initial offering and subsequent operation as a public company.

With years of experience providing IPO readiness assistance, Protiviti has developed an approach that effectively identifies key areas of focus. We provide specialized services to fit your needs, whether they include registration statement financial reporting assistance, project management, process/control remediation or systems enhancements. Our objective is to help IPO candidates avoid surprises and save time and money, as well as increase the likelihood their IPO will be timely and successful.

Contacts

Steve Hobbs
+1.415.402.6913
steve.hobbs@protiviti.com

Russ Collins
+1.469.374.2549
russ.collins@protiviti.com

Brad Rachmiel
+1.312.476.6425
brad.rachmiel@protiviti.com

Charles Soranno
+1.732.326.4518
charles.soranno@protiviti.com

protiviti®
Risk & Business Consulting.
Internal Audit.