The Impact of the Sarbanes-Oxley Act and Similar Legislation: Lessons Learned and Considerations for the Future
Protiviti, together with the input of the Singapore Accountancy Commission, has developed this point of view (POV) on the impact of the Sarbanes-Oxley Act (SOX) and similar legislation in Japan and China. Drawing upon Protiviti’s extensive experience in jurisdictions like the United States, Japan and China, this POV examines the corporate environments where strict rules were introduced through the implementation of SOX or similar legislation, the impact on internal controls of financial reporting to improve the accuracy and reliability of corporate disclosures and considerations for the future.

Against this backdrop, this POV will share practical tips and guidance learned from Protiviti’s experience in assisting companies with implementing the COSO Internal Control – Integrated Framework for compliance with the requirements of SOX and similar legislation. To complement these, discussions on SOX requirements in the United States, similar requirements in Japan and China, value propositions of SOX and similar legislation, and the cost-benefit analysis of compliance, will also be included.

It is hoped that this POV will provide the appropriate lessons learned from SOX and similar legislation that can be used in evaluating practical and cost-effective ideas for continually improving corporate governance and attracting foreign investments in Singapore.

An Important Observation

SOX and similar requirements are a part of the total fabric driving reliable financial reporting, impacted by securities laws and regulatory oversight, exchange listing requirements, accepted accounting principles, effective auditing standards, accounting firm oversight, effective standards for audit committees of boards, and independence requirements for directors and auditors, among other things. They augment the existing regulatory, governance and reporting structure and must be designed taking into consideration other legislation, rules and regulations that establish responsibility and accountability for reliable financial reporting.

I. Introduction of SOX Legislation Regimes

In the aftermath of the Enron era, several countries have enacted legislation around evaluating financial reporting controls, which require management to assess internal controls, but not the company’s external auditor. Some countries have adopted a “comply-or-explain” approach to management assessment, while others have issued corporate governance codes that recommend having a management assessment. Few countries require attestation by the external auditor, yet both the United States and Japan require an auditor attestation of internal control, while in China only management assessment of internal control is required.

United States

The United States enacted the Public Company Accounting Reform and Investor Protection Act (as titled on the Senate version of the bill) to improve public and financial reporting, commonly referred to as the Sarbanes-Oxley Act of 2002 or “SOX.” The introduction of US-SOX has spawned legislation with similar goals in other countries, most notably Japan and China. Of the numerous provisions of US-SOX, Sections 302, 404 and 906 require certification of financial statements and other financial information as well as an assertion of the effectiveness of internal control over financial reporting (ICFR) by a company’s management. In addition, Section 404 requires the issuer’s independent auditor to express an opinion on the effectiveness of ICFR as part of an integrated audit, i.e., the audit of ICFR is integrated with the audit of the financial statements. Please refer to the Appendix Part I for a more detailed discussion on the requirements of these provisions.
Japan

Japan’s version of SOX is incorporated in its Financial Instruments and Exchange (FIE) Act enacted in 2006. In applying this law, the Subcommittee on Internal Controls of the Business Accounting Council issued its “Evaluation and Auditing Standards for Internal Control for Financial Reports” and “Implementation Standards,” both of which were finalized in 2007. The Law and Standards are collectively referred to as Japanese SOX or J-SOX, and apply to companies listed on Japanese exchanges. For the Standards’ description of management’s evaluation and the audit of ICFR, please refer to the Appendix Part I. These Standards require management to develop and operate internal controls, evaluate their effectiveness and report the results in an internal control report to the public. The external auditor is also required to audit management’s evaluation of the effectiveness of internal control for financial reports.

While similar to US-SOX in many respects, there are some important differences in J-SOX that affect the process and, ultimately, the costs of conducting the management assessment and the external audit of internal controls. These differences pertain to the assessment scope for process-level controls and alignment of this scope between the external auditor and management, as well as the external auditor’s focus (i.e., the audit is focused on the appropriateness of management’s evaluation versus the effectiveness of internal control).

These requirements are elaborated in greater detail in the Appendix Part I.

China

The China stock exchanges (Shanghai stock exchange and Shenzhen stock exchange) released requirements on the disclosure of the internal control self-assessment results by listed companies in 2006. However, these were not strictly implemented due to various reasons, one of which is the lack of a common standard for assessing internal controls. Consequently, the self-assessment results brought out by companies were neither convincing nor comparable.

Later, the promulgation of the Basic Standard for Enterprise Internal Control (the Standard) in 2008 and the related series of supplemental guidelines (the Guidelines) in 2010 improved the feasibility of the stock exchanges’ requirements regarding internal control self-assessment through providing generally accepted rules for the assessment of internal control effectiveness. Together, the Standards and Guidelines are sometimes referred to as Chinese-SOX (C-SOX), which require management to undertake an annual self-assessment of internal control effectiveness and disclose the conclusion in an annual report, and apply to listed Chinese companies. Unlisted large and medium-sized Chinese companies are also encouraged to adopt the rules.

II. Value Proposition of SOX Compliance

When evaluating the value proposition of SOX, there are several related questions:

1. What is really accomplished by complying with SOX or similar regulations, i.e., what are the direct benefits?
2. Can a controls assessment accomplish more than complying with SOX or similar regulations, i.e., are there any indirect benefits?
3. What are the costs of SOX or similar regulatory compliance?

Answers to these questions will vary by country depending on what is required and whether implementation is effective. In this section of the POV, we will focus on the benefits side of the equation. Costs will be addressed in a subsequent section.
United States

Below are some direct and indirect benefits of compliance with US-SOX, based on the results of several studies. Please refer to the Appendix Part II for further details on these results.

- More Reliable Financial Reporting
- Reduced Financial Statement Restatements
- Improved Stock Price Performance
- Reduced Cost of Capital
- Continuous Improvement of Internal Processes and Control Structure

Japan

The results of an April 2013 survey by Protiviti of 175 Japanese companies on the benefits and costs of complying with the internal control-related requirements of the FIE Law and Section 404 of US-SOX showed that the following benefits were obtained through SOX compliance:

- Deeper understanding of what controls are in place and how they are operated
- Improvement in the effectiveness and efficiency of operations (e.g., process and control automation) and the further identification of duplicate and redundant controls
- Opportunity for enhancing internal audit in the areas of operational efficiency and non-financial reporting by leveraging the knowledge and experience gained through the SOX compliance.

The results are explained in further detail in Appendix Part II.

China

After several years of C-SOX practice, Chinese companies’ management are starting to realize the value of establishing and enhancing internal control systems, and have started initiatives in internal control development rather than passively complying with C-SOX. These were observed in more non-listed companies as well. Chinese companies have benefitted from implementing internal control systems under C-SOX in several ways, including, among others, improvement in the effectiveness of corporate governance structure to better support management in decision-making, enhanced efficiency in deploying resources to priority risk areas and streamlining of processes.

III. SOX and COSO

In the United States, the Securities and Exchange Commission (SEC) ruled that the criteria on which management’s evaluation of ICFR is based must be derived from a suitable, recognized control framework that is established by a body or group that has followed due process procedures, including the broad distribution of the framework for public comment.

The SEC points out in its rules that the COSO Internal Control – Integrated Framework (COSO Framework) is a “suitable framework,” and acknowledges that frameworks other than COSO that satisfy the intent of the statute without diminishing the benefits to investors may be developed within the United States in the future. Other frameworks in other countries may also meet this requirement. Please refer to the Appendix Part III(a) for more background on the COSO Framework.
Relating the COSO Framework to ICFR

The COSO Framework depicts the interrelationship among an organization’s objectives, the components of internal control, and the operating units, legal entities and other structures within the entity. Applied to ICFR, it emphasizes the importance of management’s judgment in evaluating the effectiveness of a system of internal control. Determination of effectiveness is a subjective judgment resulting from assessment of whether (1) each of the five components of internal control (as reflected in the COSO Framework) is present and functioning and (2) the five components operate together to provide “reasonable assurance” that the relevant objectives are met. The Framework facilitates this exercise of judgment by providing a total of 17 principles for the five components, upon which management exercises judgment to determine the extent to which they are present and functioning in evaluating whether the components to which these principles relate are present and functioning.

Appendix Part III(b) demonstrates how the Framework is applied to assessing the risk relating to reliable financial reporting arising from management fraud through an override of internal controls.

IV. Results of SOX Compliance

Appendix Part V provides details on studies conducted on the results of SOX compliance. A general improvement trend was noted across the United States, Japan and China.

United States

An Audit Analytics® study1 which summarized SOX results for the first six years since Section 404 went effective demonstrated the improvement in ICFR over these first years of SOX compliance in the United States, as well as a marked improvement regarding the percentage of adverse SOX 404 filings implicating a deficiency in a company’s segregation of duties.

Japan

Since the inception of J-SOX in the financial year ended March 2009, it has consistently been the case that only a small proportion of Japanese companies reported material weaknesses in their internal control systems; and this proportion is getting even smaller, reflecting the improvement and enhancement of internal controls that have taken place over the last five years.

China

Implementation of C-SOX has elevated the importance of financial reporting controls in the eyes of Chinese executives.

V. Practical Tips for Implementing the COSO Framework and Complying with SOX Requirements

Protiviti assists many companies with complying with SOX regulations and/or implementing the COSO Framework, which include listed companies as well as private companies with aspirations for going public. They also include companies of different size and scale and at different levels of internal control maturity. This section illustrates some practical tips and lessons learned that have surfaced over the years, based on our observations in assisting these companies. More details are available in the Appendix Part VI.

United States

With SOX Section 404 in play since 2004, much has been learned about what to do and what not to do.

---

1 “SOX 404 Dashboard: Year 6 Update,” Audit Analytics®, October 2010.
Use a top-down, risk-based approach – The first three years of Section 404 compliance was marred with attention to low risk areas due to a lack of standards directed to issuers. The SEC issued interpretive guidance to issuers in 2007 that promoted efficiency by allowing management to focus on those controls, i.e., “key controls,” that are needed to adequately address the risk of a material misstatement of its financial statements through a top-down, risk-based approach. Likewise, the Public Company Accounting Oversight Board (PCAOB) issued its Auditing Standard No. 5 to encourage this approach.

Apply project management concepts – As they gained experience, companies learned specific lessons in making the compliance process more effective in applying project management concepts to ensure achievement of key milestones and deadlines. More importantly, companies understood the need for top management support to be able to succeed, and involvement of external auditors at appropriate points during the process to align risk assessment considerations in order to maximize audit cost effectiveness.

Leverage on internal audit – To address the resource constraints issue so common to many companies in the first year of Section 404 compliance, internal audit proved to be a potential source of resources in documenting and testing internal controls, and providing input to management with respect to concluding on design and operating effectiveness. The COSO Framework also points out that separate evaluations conducted by internal audit serve as a form of monitoring.

Japan

The J-SOX experience offers some valuable lessons on mitigating costs of compliance for regimes considering SOX-like requirements. Based on companies surveyed, some measures that could similarly be applied include:

Reliance of external auditors on the testing performed by companies – An increase in the external auditors’ reliance on the testing performed by companies is beneficial for companies in improving the efficiency of the external audit process and raising the quality level of both internal controls and internal audit to meet the external auditor’s expectations.

Use of control self-assessment – Self-assessment methodologies facilitate allocation of the control testing workload more evenly across the company and encourage commitment of process owners to maintain and improve internal controls.

Exclude certain business locations from the scope of testing – Revisions of the J-SOX requirements now allow a rotation approach, i.e., companies may exclude a business location (such as a branch, a division and a subsidiary) from the scope of process-level controls testing, provided its controls were tested to be effective in the previous year with no significant changes in their design.

Further rationalization can be achieved by focusing on business locations where the possibility of control failure is relatively high, which can be a noteworthy point for streamlining compliance costs over the years.

Relying on the control operating effectiveness test results of the previous year – Revised J-SOX requirements also allow companies to rely on the results of testing operating effectiveness from the previous year for process-level controls to focus the overall testing effort on those controls with greater importance or with a greater possibility of failure, except for those controls considered to be of material importance in ensuring the reliability of financial reporting.
China

Protiviti’s experience with C-SOX shows that there is no “one size fits all” model of an internal control system that can be easily adopted and which still complies with C-SOX requirements. Despite that the Standards and the Guidelines are explanatory and meticulous, the internal control system of each company needs to be designed with consideration of management’s assessment of the risks, costs and benefits, and that assessment should be integrated effectively with existing policies and procedures.

VI. SOX Compliance Costs

In evaluating the value proposition of SOX, the question is usually about assessing costs versus benefits, which not only includes the benefits cited in the earlier section of this POV, but also the realization of the objective of quality financial reporting to investors through improved internal controls. In the United States, on average the costs for SOX compliance are not extraordinarily high relative to the objective of quality financial reporting.

In providing a summary on the insights on costs of compliance with the financial reporting related provisions of SOX, we acknowledge that there is no “one size fits all” model for quantifying costs. Such costs are impacted by the relative complexity of a company’s organizational structure, operating processes, information systems and accounting policies as well as the competence of its personnel, among other things.

United States and Japan

Protiviti asked 175 Japanese companies and almost 600 U.S. companies how they weighed the benefits of complying with SOX requirements relative to costs. Please refer to Appendix Part VI for more details on the responses to this 2013 survey, with a comparison to companies in the United States (surveyed in 2012). Some points to highlight from these two surveys are as below:

- More companies in the 2013 survey responded that costs associated with SOX compliance exceeded benefits. These costs also appear to be outpacing the rate of inflation and the increases are greater for the largest companies.
- The 2013 survey noted that SOX compliance costs were on the rise for many companies after several years of decline, coupled with rising external audit fees. This upward pressure is likely due to recent PCAOB guidance directing external auditors to increase the thoroughness of their internal control reviews, thereby increasing the demands auditors place on companies in providing evidence supporting their assertions on the effectiveness of ICFR.
- There was a general trend throughout the survey findings that U.S. companies may be deriving fewer benefits and value from their SOX compliance processes as compared to previous years, likely a result of the growing maturity of their control structure and compliance process.
- The majority of Japanese companies believe that costs of compliance exceed the benefits. Their ability to reap further benefits from SOX compliance appears to hinge on the extent to which they can utilize the SOX knowledge and experience in areas beyond financial reporting to bring about improvement in their broader operations.

China

While we do not have any empirical data available for China, Protiviti observed that during the first two years of compliance, companies typically devote most of their efforts and incur most of their costs with respect to the following tasks:

- Conducting a thorough review and assessment of the current status of internal controls;
Designing internal control infrastructure, e.g., policies, processes, organizational structure, reporting, methodology and systems;

Addressing and remediating a considerable number of internal control issues;

Documenting internal control standards and promoting them throughout the organization.

These tasks are practical considerations experienced by Chinese companies. Also, as compared to their counterparts in the United States and Japan, they incurred less cost in their initial years of C-SOX compliance.

VII. Lessons Learned

In closing, SOX requirements are only part of the total fabric driving reliable financial reporting. While the SOX regimes in the United States, Japan and China, as described herein, are quite different in terms of their rigor and requirements of listed companies and their external auditors, the goal of quality financial reporting is the same. In this POV, we have explored the benefits, inclusive of reliable financial reporting, and costs of SOX compliance. These are factors to consider when evaluating public policy with respect to reporting on the effectiveness of ICFR.

In sharing practical tips and lessons learned with implementing COSO and complying with SOX, this POV has also addressed the relationship between the COSO Framework and SOX compliance and provided insights regarding the SOX value proposition, how companies and investors have benefited, and the costs associated with compliance.

As we look back at the collective experiences of the United States, Japan and China, we can list 10 lessons learned from implementing SOX and similar legislation. These lessons apply to issuers, regulators and policy makers. They are provided below:

1. Make the objective as clear and focused as possible – In the early years of SOX compliance in the United States, excessive emphasis was given to determining the existence of significant deficiencies even though their existence would not affect a conclusion that ICFR was effective. The SEC issued its 2007 interpretive guidance to address this issue by altering the definition of a “significant deficiency” and clarifying the focus on identifying the existence of a “material weakness.”

2. Apply a top-down, risk-based approach – In the early years of SOX compliance in the United States, there was excessive attention given to controls in low risk areas. In another topic in the SEC 2007 interpretive guidance, the SEC staff clarified that the approach issuers should use must be risk-based and should consider entity-level controls (i.e., top-down). Likewise, the PCAOB clarified the need for a top-down, risk-based approach by the external auditor.

3. Source the risk of potential material misstatements – Management must understand the flow of transactions related to relevant financial reporting elements and assertions, including how these transactions are initiated, authorized, processed and recorded. Using that understanding, all points within the company’s processes at which risks of a material misstatement could arise should be identified. Controls that management has implemented to address these potential risks are then identified – these are the so-called “key controls.” For example, these risks might include unauthorized acquisition, use or disposition of the company’s assets that could result in a material misstatement of the financial statements.

4. Perform an adequate fraud risk assessment – In sourcing risk, it is important to note that misstatements in the financial statements can arise from either fraud or error. The distinguishing factor between fraud and error is whether the underlying action that results in misstated financial statements is intentional or unintentional. More important, a system of internal control can be circumvented if people collude or if management is able to
override controls. Even though an entity’s system of internal control should be designed to prevent and detect collusion, human error, and management override, there is no absolute assurance that an effective system of internal control cannot experience failure. That is why the risk of fraud should be assessed in conjunction with sourcing financial reporting risk.

5. **The number of key controls is the primary cost driver** — This lesson became apparent after a few years of implementation in the United States. At that point, companies began rationalizing their compliance scope applying a top-down, risk-based approach to reduce the controls population down to the ones that really matter in reducing the risk of material errors and omissions in the financial statements to an acceptable level.

6. **Documentation of the risks and controls that matter is an essential part of the process** — The documentation supporting management’s assessment does not need to include the entire population of controls that exists within a process that impacts financial reporting. Such documentation should be focused only on those controls that management concludes are adequate to address the identified financial reporting risks. Evidential matter arising from both the design process and the testing process must provide reasonable support for management’s assertion regarding the effectiveness of the company’s key financial reporting controls. Developing and maintaining such evidential matter is an inherent aspect of an effective system of internal controls.

7. **Pay attention to “tone at the top”** — The right culture is an important prerequisite to a strong system of internal control. That is why the control environment, which is one of the components of the COSO Framework, should be in place and operating effectively. The control environment lays the foundation for a strong system of internal control.

8. **Ensure objectivity and competency of evaluators testing controls in high-risk areas** — The use of internal audit and other objective and competent personnel provides management with sufficient evidential matter to support a conclusion on the effectiveness of internal control. In addition, the external auditor is able to increase reliance on the work of others when performed by objective and competent evaluators.

9. **Encourage an environment of continuous improvement in financial reporting controls** — Even world-class organizations have discovered the need to improve their internal control over financial reporting continuously. In addition to reducing the number of key controls, many companies leveraged and took advantage of automated controls and monitoring processes. Coupled with self-assessment methodologies, both controls automation and monitoring activities increased the transparency into how the control environment is operating.

10. **Bring to bear project management discipline to this compliance activity until it can be transitioned to a process** — For large, complex organization, initial adoption of a rigorous evaluation of financial reporting controls is a major project requiring a project management office (PMO) type discipline. The project should be organized with a clear road map with appropriate milestones and checkpoints. Companies should work closely with their accounting firm, if attestation is required, and obtain input as to scope, approach and expectations. Technology should be used to manage the process, reporting and data, and may be vital to transitioning the compliance project to an ongoing process. Control activities that are not being applied correctly should be identified timely (i.e., “fail the testing process” when it is evident the control is not performing), control deviations and deficiencies should be assessed on a timely basis and significant deficiencies remediated timely.
Appendix

I. INTRODUCTION OF SOX LEGISLATION REGIMES – REQUIREMENTS

United States

Specific Requirements of Sections 302, 404 and 906 of US-SOX

- **Section 302** – This provision of SOX requires a company’s principal executive officer or officers and the principal financial officer or officers, or persons performing similar functions, to certify each quarterly or annual report and make certain disclosures. Specifically, they must state that they have reviewed the report and, based on their knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made therein, in light of the circumstances under which they were made, not misleading with respect to the reporting period. They must also state that, based on their knowledge, the financial statements and other financial information in the report fairly present in all material respects the financial condition, results of operations and cash flows of the company as of, and for, the periods presented in the report. Finally, they must acknowledge that they are responsible for establishing and maintaining “disclosure controls and procedures” and “internal control over financial reporting” for the issuer and have:
  - Designed such disclosure controls and procedures (DCP), or caused such DCP to be designed under their supervision, to ensure that material information is made known to them, particularly during the period in which the periodic report is being prepared;
  - Designed internal control over financial reporting (ICFR), or caused such ICFR to be designed under their supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;
  - Evaluated the effectiveness of the issuer’s DCP as of the end of the period covered by the report, and have presented in the report their conclusions about the effectiveness of the DCP based on their evaluation;
  - Disclosed in the report any change in the issuer’s ICFR that occurred during the issuer’s most recent fiscal quarter (the “fourth fiscal quarter” in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the issuer’s ICFR; and
  - Disclosed, based on their most recent evaluation of ICFR, to the auditors and to the audit committee:
    - All significant deficiencies and material weaknesses in the design or operation of ICFR that are reasonably likely to adversely affect the company’s ability to record, process, summarize and report financial information; and
    - Any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer’s internal control over financial reporting.

Section 302 certifications apply to companies filing quarterly and annual reports with the Securities & Exchange Commission (SEC) under either Section 13(a) or 15(d) of the Exchange Act. Such certifications are required effective immediately once a company goes public. For most companies, the certifying officers are the CEO and CFO. While companies have the flexibility to have others sign the certification in addition to the CEO and CFO if they determine it is appropriate to do so because of the
extent of their involvement in the financial reporting and disclosure process, we have rarely seen this happen.

- **Section 404** – Section 404(a) of SOX requires management to issue an annual internal control report to articulate (a) management’s responsibilities to establish and maintain adequate ICFR, (b) the framework used by management as the basis for evaluating the effectiveness of internal control, and (c) management’s conclusions as to the design and operational effectiveness of ICFR based on management’s year-end evaluation (i.e., a point-in-time assessment), including disclosure of any material weaknesses in the company’s internal controls identified by management. The internal control report must be included in the issuer’s annual report. In addition, Section 404(b) requires the issuer’s independent auditor to express an opinion on the effectiveness of ICFR. The internal control report of Section 404(a) is required of all public companies, whereas the attestation report of Section 404(b) is required of companies meeting the requirements of an “accelerated filer” which means, among other things, they have a market capitalization of at least US$75 million (defined as public float).

- **Section 906** – This SOX provision requires a separate certification from the one required by Section 302. The Section 906 certification requirement differs from Section 302 in at least three respects:
  - Section 906 expressly imposes criminal penalties, whereas Section 302 relies on the general criminal penalty provision that applies to all violations of the Exchange Act.
  - The Section 906 certification is a shorter representation basically stating that the periodic report containing the financial statements fully complies with the requirements of Section 13(a) or 15(d) of the Exchange Act, and that the information contained in the periodic report fairly presents, in all material respects, the financial condition and results of operations of the issuer.
  - Unlike the Section 302 certifications, the Section 906 certifications are required only in periodic reports that contain financial statements.

The two sets of certification requirements under Sections 302 and 906 surfaced from different facets of the legislative process. Both are required even though they overlap significantly. A fraudulent Section 302 certification is subject to civil enforcement by the United States Securities & Exchange Commission (SEC), and a fraudulent Section 906 certification carries criminal penalties enforceable by the United States Department of Justice. The comprehensive evaluations and assessments required of the certifying officers under Section 302 also should enable these officers to sign the certification required by Section 906.

**Top-Down, Risk-Based Approach**

Specifically in the implementation of Section 404, the SEC in its Interpretive Guidance Regarding Management’s Report on Internal Control Over Financial Reporting and Public Company Accounting Oversight Board (PCAOB) in its Auditing Standard No. 5 have encouraged a top-down, risk-based approach as the most practical way to evaluate internal controls.

This approach focuses the evaluation process on several key decisions early in the process, beginning with selecting the most significant captions and disclosures from the financial statements. These captions and disclosures, and the significant accounts supporting them, represent the priority financial reporting elements. That accomplished, the project team then identifies the financial reporting assertion risks relevant to each significant financial reporting element and sources these risks within the major transaction flows that impact the priority financial reporting elements (sourcing the risks requires an understanding of the major transaction flows).

A-2
Once the risks are sourced, the evaluation team then selects the key controls that address the most critical financial reporting assertions and evaluates the effectiveness of their design. This approach also (a) considers the relative risk levels (including the risk of control failure) when deciding the evidence needed to support a conclusion regarding the effectiveness of controls operation, (b) determines multi-location scoping considerations based on risk, and (c) sets documentation standards appropriate to different levels of risk.

Japan

Description of Management’s Evaluation and Audit of ICFR

- **Evaluation of and Reporting on Internal Control for Financial Reports** – Management assumes the role and responsibility to develop and operate internal controls, and is required to evaluate the effectiveness of internal control for financial reports, and report the results in the form of an internal control report to the public. In order to evaluate the effectiveness of internal controls, management must first evaluate internal controls that have a significant and pervasive impact on the financial reports as a whole (companywide internal control). Management must then evaluate the internal controls relating to specific processes. The scope of the review of specific processes would be based on the results of the evaluation of the companywide controls.

- **Audit of Internal Control for Financial Reports** – The external auditor responsible for auditing the company’s financial statements also must conduct an audit of management’s evaluation of the effectiveness of internal control for financial reports. The objective of the audit is to determine the appropriateness of management’s evaluation. The external auditor compiles the audit results in the form of an internal control report and submits it to management.

Differences between J-SOX and US-SOX

- **Assessment scope for process-level controls** – Under J-SOX, the requirement is to include in the assessment scope for process-level controls at least two-thirds of the business locations (such as branches, divisions and subsidiaries) comprising a corporate group (in terms of consolidated revenue or some other appropriate accounting metric), whereas under US-SOX the requirement for multi-location coverage is more rigorous. Also, under J-SOX, it is required that companies include in the assessment scope for process-level controls those business processes that significantly affect financial statement items that are closely related to their business objectives; and for a typical company, the significant financial statement items are defined as revenue, accounts receivable, and inventory. In addition to the business processes affecting these three financial statement items, companies are required to add to the assessment scope those business processes that are considered to be significant because, for example, they involve high-risk transactions, accounting estimates or forecasts, or non-routine or non-standardized transactions. As a result of these specific requirements, it is generally the case that the assessment scope for process-level controls under J-SOX is narrower than that under US-SOX.

- **Adoption of “indirect reporting”** – Unlike US-SOX, the external auditor under J-SOX does not directly assess the design and operating effectiveness of internal controls. Instead, the external auditor assesses whether management’s assessment of internal controls has been performed in a proper manner. According to the Financial Services Agency of Japan, this distinction in approach makes the external audit more efficient by ensuring that the assessment scope for management is the same as the assessment scope for the external auditor; therefore, the external auditor does not expand the assessment scope on its own.
Integration of internal control audit with financial statement audit – It is the requirement of J-SOX that, in principle, the audit of internal controls and the audit of financial statements must be conducted by the same external auditor (the “same external auditor” means the engagement partner for the internal control audit and the financial statement audit is the one and the same individual). The requirement is intended to enhance the efficiency of external audit by allowing the use of the same set of evidence for both internal control audit purposes and financial statement audit purposes. While no such requirement exists under US-SOX, from a practical standpoint the audit firms conduct the integrated audit, as required by Auditing Standard No. 5, in this manner.

China

The Basic Standard for Enterprise Internal Control (the Standard) in 2008 and the related series of supplemental guidelines (the Guidelines) in 2010 are formulated and published by the Ministry of Finance together with the China Securities Regulatory Commission CSRC, the National Audit Office, the China Regulatory Commission and the China Insurance Regulatory Commission. Together, the Standards and Guidelines are sometimes referred to as Chinese-SOX (C-SOX), which apply to listed Chinese companies, which have improved the feasibility of the stock exchanges’ requirements regarding internal control self-assessment through providing generally accepted rules for the assessment of internal controls effectiveness. Unlisted large and medium-sized Chinese companies are also encouraged to adopt the rules.

C-SOX requires management to undertake an annual self-assessment of internal control effectiveness and disclose the conclusion in an annual report. C-SOX aims to provide clear guidelines for Chinese companies to systematically enhance their internal control system to provide reasonable assurance on such objectives as legal compliance, asset safety, reporting accuracy and completeness, operational efficiency and effectiveness, and strategy realization. The Standards and Guidelines are designed with reference to the COSO Framework, whereas the internal control objectives of C-SOX are extended to include “strategy realization” and “asset safety” according to Chinese enterprises’ local management situation.

Since its release, most listed companies have complied with C-SOX. Besides State-owned Assets Supervision and Administration Commission of the State Council (SASAC), shareholders of many large state-owned companies also require subordinated companies to comply with C-SOX with a focus on risk and fraud prevention despite their listing status.

II. VALUE PROPOSITION OF SOX COMPLIANCE – RESULTS

United States

More Reliable Financial Reporting – In its 2011 Study and Recommendations on Section 404(b) of the Sarbanes-Oxley Act of 2002 “For Issuers With Public Float Between $75 and $250 Million," the SEC concluded that “financial reporting is more reliable when the auditor is involved with ICFR assessments” and "investors generally view the auditor's attestation on ICFR as beneficial." The study found evidence that auditor testing of ICFR has generally resulted in the disclosure of control deficiencies that were not previously disclosed by management. The study also noted the following:

- Auditor testing appears to have a positive effect on the quality of financial reporting generally.
- Issuers that only filed Section 404(a) reports – that is, the management certification in the annual internal control report, without 404(b) auditor attestation – were significantly more likely to restate their financial
statements than issuers that complied with both Section 404(a) and Section 404(b).

**Commentary:** Section 404 has two sub-paragraphs. Section 404(a) requires ALL listed companies to include a management report on an annual basis addressing the effectiveness of ICFR. Section 404(b) requires the independent auditor of all companies classified as accelerated filers or large accelerated filers to express an opinion on the effectiveness of ICFR. The SEC’s study contrasted the experience of non-accelerated filers who must only comply with Section 404(a) with the experience of the accelerated filers complying with both Section 404(a) and Section 404(b). Protiviti's experience is that the involvement of the external auditor in the process increases the rigor of the compliance process. If a top-down, risk-based approach is applied, the interaction between management and the auditor on the relevant financial reporting assertions, critical risk areas, key controls, testing results and reporting requirements keeps the process focused.

- **Reduced Financial Statement Restatements** – One measure of benefits is the trend line in restated financial statements over time. In March 2013, Audit Analytics® published a research report, “2012 Financial Restatements: a Twelve Year Comparison.” The report states that its findings were based on data from more than 12,000 financial restatements and/or non-reliance filings disclosed by over 7,000 SEC public registrants since January 1, 2001.

  The report notes the following findings:
  - The number of restatement and non-reliance disclosures peaked in 2006 with 1,771 disclosures. In each of the three following years, the number of disclosures declined with 715 restatements in 2009. After this period of decline, restatements increased slightly for two years and, in 2012, declined again to 768. Audit Analytics® described the number of restatements over the four-year period from 2009 until 2012 as “relatively stable.”
  - While the number of restatement and non-reliance disclosures appears to have levelled off in 2012, indicators of severity show that the incidents disclosed in 2012 were generally lower in severity, with some indicators achieving the most favourable value for all the 12 years under review.
  - In evaluating the breakdown by company size, Audit Analytics® used filer status (e.g., non-accelerated versus accelerated filers). While total restatements levelled off, the number of restatements from accelerated filers increased for the third straight year. To illustrate: In 2009, a total of 153 U.S. accelerated filers disclosed restatements. In 2010, the number increased to 158 restatements followed by 202 and 245 in 2011 and 2012, respectively.

**Commentary:** This important research indicates that the quality of public reporting has improved since the Sarbanes-Oxley legislation was enacted 12 years ago. While one cannot pinpoint the exact drivers of this improved performance, it is reasonable to assert that one of the causal factors is compliance with Sections 302, 404 and 906. Sections 302 and 906 establish clear responsibility for fair financial

---

2 There are some temporary exemptions, such as a newly public company or company qualifying under The Jumpstart Our Business Startup Act (JOBS Act).

3 “Non-reliance” is a “reportable event,” as defined by the United States SEC, occurring when an issuer determines that a past financial statement should no longer be relied upon. While not a restatement, a non-reliance disclosure is a serious matter which often leads to a restatement. For purposes of its research, Audit Analytics® combined restatement and non-reliance disclosures.

4 When reviewing the adverse effect of the restatements, Audit Analytics® used the following criteria: (1) the negative impact on net income, (2) the average cumulative impact on net income per restatement, (3) the percentage of restatements with no impact on income statements, (4) the average number of days restated, and (5) the average number of issues identified in the restatements.
reporting. Section 404 compliance further supports financial reporting. The existence or absence of a material weakness in ICFR is a measure of the reliability of financial reporting. If a material weakness exists, it presents a higher risk of misstated financial statements and subsequent restatements. The identification of key risk areas in the Section 404 compliance process facilitates the improvement of critical processes and controls and the certifying officers to drive accountability throughout the organization, both of which reduce financial reporting risk.

- **Improved Stock Price Performance** – A study released in May of 2006 by Lord & Benoit reported that shareholders benefit when companies have effective ICFR. To illustrate, for the period from March 31, 2004 to March 31, 2006, the Russell 3000 share index increased by 17.7 percent. The Lord & Benoit study found that companies reporting no material weaknesses in ICFR for either 2004 or 2005 enjoyed a 27.7 percent increase in share price. Companies reporting material weaknesses in 2004 but no material weaknesses in 2005 experienced a 25.7 percent increase in share price. However, companies reporting material weaknesses in both 2004 and 2005 suffered a 5.7 percent decline in share price. Therefore, the companies that reported that their ICFR was ineffective both years experienced poorer performance in their stock price relative to the companies that did not.

**Commentary:** The Lord & Benoit study results suggest that companies that reported no material weaknesses in ICFR or demonstrated diligence in remediating a reported material weakness are rewarded with superior stock price performance compared to companies that continue to report unremediated material weaknesses.

- **Reduced Cost of Capital** – In a research paper co-authored by several noted academics, the authors concluded that while SOX mandated management evaluations and independent audits of ICFR effectiveness were costly to issuers, they may yield benefits through lower information risk that translates into lower cost of equity. The study methodology used unaudited pre-SOX Section 404 disclosures and SOX Section 404 audit opinions to assess how changes in internal control quality affect firm risk and cost of equity by controlling for other risk factors. We find that firms with internal control deficiencies have significantly higher idiosyncratic risk (meaning a propensity to act or behave in an unusual way), systematic risk and cost of equity. The authors noted that “auditor-confirmed changes in internal control effectiveness (including remediation of previously disclosed internal control deficiencies) are followed by significant changes in the cost of equity that range from 50 to 150 basis points.”

**Commentary:** These findings are similar in substance to the results in the Lord & Benoit study, which suggested that assertions in internal control reports affected how investors assessed risk. In turn, this assessment forces downward pressure on the issuer’s stock and increases the issuer’s cost of equity.

- **Continuous Improvement of Internal Processes and Control Structure** – For several years, Protiviti has conducted annual surveys of representatives from companies listed on U.S. exchanges to obtain their views on the SOX compliance process, including its costs and value. In 2013, Protiviti surveyed nearly 300 executives. Consistent with the results from 2012, 6 out of 10 executives believed

---

that his or her organization currently leveraged Sarbanes-Oxley compliance efforts to drive continuous improvement of business processes that affect financial reporting. The results showed that the larger the company, the more likely the view that SOX compliance contributed to continuous process improvement. In the survey, Protiviti asked the question, "What are the primary benefits your organization expects to achieve in the coming fiscal year through Sarbanes-Oxley compliance?" The participants responded as follows (with the percentage responding noted parenthetically):

- Enhanced understanding of control design and control operating effectiveness (46%)
- Increased effectiveness and efficiency of operations (43%)
- Internal audit is able to perform more traditional audits in operational and non-financial reporting related areas (40%)
- Ability to better identify duplicate and superfluous controls (35%)
- Reduced Section 404(b) and Section 302 compliance costs (25%)
- No benefit – simply complying with SEC requirements (13%)

These results illustrate that SOX compliance can have important indirect benefits beyond compliance with the SEC’s reporting regulations.

**Commentary:** As in prior surveys, organizations continue to report improvements in their internal control structures as well as opportunities to improve processes. Protiviti sees continued opportunities, particularly with respect to automation of controls. Almost nine in 10 companies reported benefits.

**Japan**

Most of the companies surveyed are those listed on stock exchanges in Japan and are therefore complying with the requirements of FIE. Some of these listed companies (accounting for 10 percent of the surveyed companies) are also SEC registrants and are thus complying with the requirements of Section 404 of the Sarbanes-Oxley Act as well. A small number of the companies surveyed (6 percent) are not listed companies and are therefore complying with such requirements on a voluntary basis. For purposes of presenting the survey results, these requirements are collectively referred to as the “SOX requirements.” The findings regarding the benefits of complying with the SOX requirements are summarized below.

We asked the surveyed companies the following question: What benefits can be expected to be obtained from complying with the SOX requirements in the coming few years? The participants responded as follows (with the percentage responding noted parenthetically):

- Deeper understanding of control design and control operating effectiveness (79%)
- Further identify duplicate and superfluous controls (50%)
- Increased effectiveness and efficiency of operations (46%)
- Internal audit is able to perform more traditional audits in operational and non-financial reporting related areas (45%)
- Further reduce SOX compliance costs (34%)
- Promote process and control automation (34%)
- No particular benefits beyond meeting minimum SOX requirements (30%)

As a result of SOX compliance, almost four in five companies believe that through SOX compliance, they can gain a deeper understanding of what controls are in place and
how they are operated. As in the United States, we noted that this benefit is one that can be naturally obtained in the course of conducting the management assessment of internal controls. But there is one important difference: In the United States, companies are more mature in their SOX compliance and therefore, fewer companies (46 percent) see the benefit of further understanding of their controls than in Japan.

It is noteworthy that half the companies view the improvement of the effectiveness and efficiency of operations and the further identification of duplicate and redundant controls as benefits that can arise from SOX compliance. These benefits will not be obtained by merely complying with SOX requirements, but only by making a conscious effort to turn findings from the internal control assessment into specific actionable opportunities for improving broader operations and making controls more efficient.

Finally, nearly half the companies see an opportunity for enhancing internal audit in the areas of operational efficiency and non-financial reporting by leveraging the knowledge and experience gained through SOX compliance.

**China**

Benefits of implementing internal control systems under C-SOX:

- Improved the effectiveness of the corporate governance structure to better support management’s decision-making processes;
- Adopted “risk-based” internal control mechanisms to assist management in effectively deploying limited internal control resources according to the priority risks;
- Established proper authorization and delegation of duties to reduce risk and to streamline excessive approval processes;
- Improved maturity level of internal controls from “ad-hoc reaction” to a more systematic process and emphasis on active prevention; and
- Identified and remediated IT general control weaknesses, and raised management’s attention toward IT-related risks.

### III. (a) SOX AND COSO – THE COSO FRAMEWORK

The SEC’s definition of a “suitable framework” on which management’s evaluation of ICFR is based must:

1. Be free from bias;
2. Permit reasonably consistent qualitative and quantitative measurements of a company’s internal control;
3. Be sufficiently complete so that those relevant factors that would alter a conclusion about the effectiveness of a company’s internal controls are not omitted; and
4. Be relevant to an evaluation of internal control over financial reporting.

COSO stands for “Committee of Sponsoring Organizations of the Treadway Commission” and is a voluntary private-sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls and corporate governance. COSO was originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private sector initiative often referred to as the Treadway Commission. The Commission studied the causal factors that can lead to fraudulent financial reporting and developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions.
The sponsoring organizations are the American Institute of Certified Public Accountants (AICPA), The Institute of Internal Auditors (IIA), Financial Executives International (FEI), Institute of Management Accountants (IMA) and the American Accounting Association (AAA). COSO so far has produced four documents: one in 1992 on the Internal Control – Integrated Framework, which it updated in 2013; one in the mid-1990s on derivatives; one in 2004 on the Enterprise Risk Management – Integrated Framework; and one in 2005 to provide guidance to smaller public companies applying the integrated internal controls framework to report on internal control over financial reporting, which was updated in 2009 to provide guidance on monitoring. Over the last four years, in addition to updating the Internal Control Framework, COSO has commissioned several research projects and thought papers on a variety of topics.

Ever since US-SOX was issued, the original 1992 version of the Internal Control Framework 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 ICFR by public companies listed in the United States. It is also commonly used for other similar regulatory requirements outside the United States, including J-SOX.

The updated 2013 Internal Control – Integrated Framework was driven by the intent to benefit from the experience over the period since the original 1992 Framework was issued. It will supersede the 1992 original version by December 15, 2014.

The 2013 Internal Control – Integrated Framework defines internal control as follows:

Internal control is a process, effected by an entity’s board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

The update Framework retains the three dimensional cube introduced by the 1992 original. As seen below, the cube begins with objectives along the top relating to operations, reporting and compliance, representing the cube’s columns. Every organization establishes relevant objectives and formulates strategies and plans for achieving them. The side of the cube, as shown below, depicts that objectives may be set for the entity as a whole, or be targeted to specific divisions, operating units and functions within the entity (including business processes such as sales, purchasing and production), illustrating the hierarchical top-down structure of most organizations.

![Diagram of COSO Internal Control Framework](source: Chapter 2 of the 2013 COSO Internal Control: Integrated Framework)
On the face of the cube are the five components of internal control, representing the rows of the cube. These components support the organization in its efforts to achieve its objectives. The five components are Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities. They are relevant to an entire entity, meaning they operate at the entity level, as well as at all divisions, operating units, functions, subsidiaries or other subsets of the entity.

The above cube depicts the direct relationship among the organization’s objectives (which are what the entity strives to achieve); the components of internal control (which represent what is needed to achieve the objectives); and the operating units, legal entities and other structures within the entity (which are the levels of the organization where the components of internal control operate). Each internal control component cuts across and applies to all three categories of objectives.

Applied to ICFR, the Framework recognizes that external financial reporting is an objective falling in the “Reporting” category. The effectiveness of internal control is assessed, using a principles-based approach, relative to the five components of internal control. To have an effective system of internal control relating to ICFR, all five components must be present, functioning and operating together. For example, when considering internal control over a particular financial reporting objective, all five components must be present, functioning and operating together in order to conclude that internal control relating to the financial reporting objective is effective.

The COSO Framework emphasizes the importance of management’s judgment in evaluating the effectiveness of a system of internal control. Determining whether a particular internal control system is effective is a subjective judgment resulting from an assessment of whether each of the five components of internal control is present and functioning, and that the five components of internal control operate together to provide “reasonable assurance” the relevant objectives are met. To facilitate this exercise of judgment, the Framework provides principles for each of the five components of internal control, 17 principles in all. Management exercises judgment in determining the extent to which these principles are present and functioning when evaluating whether the components to which the principles relate are present and functioning.

IV. (b) SOX AND COSO – A PRACTICAL EXAMPLE

{
Preventing Senior Management Fraud

One of the risks to reliable financial reporting is the issue of management fraud, which can arise as a result of management override of internal control. The five principles underlying the Control Environment component facilitate the tone at the top that provides checks and balances in dealing with this issue. The COSO Framework states that if management is able to override controls, the entire system may fail.

Principle 2 of the Framework states:

The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

In providing oversight for the system of internal control, the board of directors retains oversight responsibility for management’s design, implementation, and conduct of internal control. This includes overseeing management’s assessment of risks to the achievement of objectives, including the potential impact of significant changes, fraud, and management override of internal control.

The COSO Framework states the following:

Management override describes action taken to override an entity’s controls for an illegitimate purpose including personal gain or an enhanced presentation of an entity’s financial condition or compliance status. For example, to allow a large
shipment of goods to a customer with unacceptable credit in order to increase revenue, a manager improperly overrides internal control by approving the sale transaction placed on credit hold by a supervisor who conducted the control properly. Actions to override are typically not documented or disclosed, because the intent is to cover up the actions.

Management override should not be confused with management intervention, which represents action that departs from controls designed for legitimate purposes. At times, management intervention is necessary to deal with non-recurring and non-standard transactions or events that otherwise might be handled inappropriately. Providing for management intervention is necessary because controls cannot be designed to anticipate and mitigate every risk. Management’s actions to intervene are generally overt and documented or otherwise disclosed to appropriate personnel.

As part of assessing fraud risk, management assesses the risk of management override of internal control. The board of directors or subset of the board (e.g., audit committee) oversees this assessment and challenges management depending on the circumstances. The entity’s control environment can significantly influence the risk of management override. This is especially important for smaller entities where senior management may be very involved in conducting many controls.

Another factor is segregation of duties, which can address important risks relating to management override. Segregation of duties is fundamental to mitigating fraud risks because it reduces the risk of a single person acting alone. However, there is always the risk that management can override control activities. Collusion is needed to perform fraudulent activities when key process responsibilities around authorization, execution and asset custody are divided among different employees.

Principle 8 in the COSO Framework relates to fraud:

The organization considers the potential for fraud in assessing risks to the achievement of objectives.

In the United States, many companies integrated their evaluation of the effectiveness of controls mitigating fraud risk with the evaluation of other controls embedded within the organization’s processes. The underlying premise is that control activities are an integral part of making business processes work. Embedded within the processes, they provide assurance that the processes are preventing and detecting on a timely basis errors and fraud as close as possible to the source, providing assurance that relevant financial reporting assertions are met. Control activities are in place within the process to reduce financial reporting risks to an acceptable level, including the risk of fraud. The financial reporting assertions and the risks (“what can go wrong”) to achieving those assertions provide a context for evaluating the design effectiveness of control activities at the process level. Fraud risk is often worked into the identification of the risks; therefore, many companies in the United States embed their assessment of fraud risk into their overall assessment of financial reporting risk.Protiviti and, to the best of our knowledge, most of the accounting firms have supported this integrated approach, provided that fraud scenarios common to the company’s industry are appropriately considered.
V. RESULTS OF SOX COMPLIANCE

United States

In another Audit Analytics® study, SOX results were summarized for the first six years since Section 404 went effective. The study reported the following findings:

- With respect to Year 6 (Calendar 2009 and fiscal years ended in 2010 through June 2, 2010), the SEC had received a total of 3,356 auditor attestation opinions and 3,066 management-only opinions (6,422 in total).

- The adverse auditor attestation disclosures filed represented 2.4 percent of the attestation filings received to date. This figure was expected to increase to about 2.8 percent, assuming that overdue filings disclose adverse conditions. It was also reported that the 2.8 percent figure could further increase as some companies ascertain, mostly through financial restatements, that they erred in the original assessment that ICFR was effective.

- The adverse figure of 2.8 percent is the lowest disclosed to date, down from 5.0 percent in Year 5; 7.7 percent in Year 4; 9.1 percent in Year 3; 10.3 percent in Year 2 and 16.9 percent in Year 1.

- The management-only assessments also showed improvement. The adverse disclosures in the management-only assessments represented 27.8 percent of those filed. This is the first time the figure was below 30 percent, with the prior three years experiencing the following adverse percentage rates: 32.3 percent in Year 5; 32.0 percent in Year 4 and 32.8 percent in Year 3.

The above results provided by the Audit Analytics® study demonstrate that, over the first six years of SOX compliance in the United States, ICFR improved. Other findings were as follows:

- In Year 6 the adverse auditor attestations filed by first-time accelerated filers were the lowest percentage rate to date, demonstrating that the experience curve reflected improvement.

- Since Section 404’s implementation, accelerated filers have experienced a marked improvement regarding the percentage of adverse SOX 404 filings implicating a deficiency in a company’s segregation of duties. To illustrate, deficiencies in a company’s segregation of duties were noted in 23.9% of the adverse filings in Year 1, but only 11.0% of adverse filings in Year 6.

- In Year 6, the most common internal control issues disclosed were material year-end adjustments, personnel issues, IT processing and access issues, financial restatements, segregation of duties and internal audit issues.

Japan

For the period from March 2009 to February 2010, 3,795 companies that submitted internal control assessment reports and 92, or 2.4 percent, of those companies reported material weaknesses. For the same period for the next four years, the percentage of companies reporting material weaknesses in their originally filed reports declined as follows:

- For the 12 months ended February 2011 .9 percent
- For the 12 months ended February 2012 .4 percent
- For the 12 months ended February 2013 .6 percent

---

7 “SOX 404 Dashboard: Year 6 Update,” Audit Analytics®, October 2010.
For the 12 months ended February 2014 0.2 percent

Some companies originally submitted internal control assessment reports asserting that there were no material weaknesses in their internal control systems subsequently identified material weaknesses and restated their internal control assessment reports. The number of companies reporting material weaknesses in restated internal control assessment reports was eight, 12, 15 and 20 for the 12 months ended May 2010, 2011, 2012 and 2013, respectively.

VI. PRACTICAL TIPS ON COMPLIANCE WITH SOX REQUIREMENTS

United States

With SOX Section 404 in play since 2004, much has been learned about what to do and what not to do. Following is a simple illustration of the sequence of steps in complying with Section 404.

It is very important to apply the above approach using a top-down, risk-based approach. In the United States, the first three years of Section 404 compliance were marred with attention to low risk areas due to a demanding audit standard issued by the PCAOB. Management of issuers was compelled to follow the audit standard because there were no standards provided by the SEC to issuers. To address the need for a more efficient compliance process, the SEC issued interpretive guidance to issuers in 2007. This guidance was organized around two broad principles:

1. Management should use a top-down, risk-based approach to evaluate whether it has implemented controls that adequately address the risk that a material misstatement of the financial statements would not be prevented or detected in a timely manner. A top-down, risk-based approach includes the role of entity-level controls in assessing financial reporting risks and the adequacy of controls.

2. Management’s evaluation of evidence about the operation of its controls should be based on its assessment of risk. The guidance provides an approach for making

---

8 This is for companies having reported thus far.

risk-based judgments about the evidence needed for the evaluation, allowing management to align the nature and extent of its evaluation procedures with those areas of financial reporting that pose the highest risks to reliable financial reporting. As a result, management may be able to use more efficient approaches to gathering evidence, such as self-assessments, in low-risk areas and perform more extensive testing in high-risk areas.

The SEC’s guidance promoted efficiency by allowing management to focus on those controls that are needed to address adequately the risk of a material misstatement of its financial statements. The guidance does not require management to identify every control in a process or document the business processes impacting ICFR. Rather, management can focus its evaluation process and the documentation supporting the assessment on those controls that it determines adequately address the risk of a material misstatement of the financial statements. These are what are commonly referred to as the “key controls.”

The PCAOB updated its audit standard to reflect a top-down, risk-based approach consistent with the SEC’s guidance.

Companies also learned specific lessons in making the compliance process effective. For many companies, the initial year of compliance was a major project. After the initial year, the project evolved to an ongoing process. Some of the key lessons relating to planning, organizing and managing the project are as follows:

- The first year of compliance is often a challenge – for everyone. For most first adopters, the Section 404 compliance effort is a major project effort requiring a project management office (PMO) type of discipline to ensure that key milestones and deadlines are met.
- Top management support of the effort is vital; it is difficult to succeed without it.
- Operating unit managers and process owners (both in-house and outsourced) must be involved and held accountable as many individuals responsible for key controls report to them. Therefore, senior management must communicate everyone’s role up, down, across and outside the organization and monitor progress through the assistance of the PMO or project manager.
- It is critical to take charge of the project, and avoid such pitfalls as managing the project at too low a level within the organization, letting the project team get lost in irrelevant details and low risk areas and allowing key scoping decisions to remain unaddressed too long.
- The Section 404 assessment is a point-in-time assessment, meaning the effectiveness of ICFR is evaluated as of the end of the year. Therefore, if there are any internal control deficiencies, the issuer has an opportunity to remediate them prior to the end of the year. It is critical, however, that such remediation be completed timely enough to enable sufficient testing of operational effectiveness. That is why it is important to begin the effort early enough to permit remediation and retesting.
- Involve the external auditor at appropriate points during the process. Work with them, understand their needs and timing requirements, conduct periodic checkpoints and plan to give them sufficient time to complete their work. Following are eight critical risk assessment considerations to checkpoint with the auditor:
  1. Select significant financial reporting elements
  2. Identify relevant assertions for each significant financial reporting element
  3. Understand major transaction flows
(4) Source risks of material misstatements within major transaction flows
(5) Select effectively designed key controls addressing each relevant assertion
(6) Decide documentation standards at different levels of risk
(7) Consider relative risk levels to decide tests of operating effectiveness
(8) Determine locations and units to include into scope

The above considerations are important to driving the efficiency of the process. The SEC’s interpretive guidance allows management to exercise judgment during the risk assessment and scoping process on these matters using a top-down, risk-based approach. The decisions management makes in conjunction with the above considerations provide a context for management’s dialogue with the external auditor during the early stages of the process. The external auditor’s application of a top-down, risk-based approach is greatly augmented by, and reaches the highest level of efficiency when the auditor understands, a well-documented management application of that approach, as evidenced by management’s consideration of the above matters.

There is another vitally important reason why the eight risk assessment considerations are so important. If management and the external auditor can agree on the key decisions addressed through these matters, it leaves open one remaining critical decision – the scope for testing the operating effectiveness of the key controls. This particular decision is the most natural point of divergence between management and the auditor in their respective evaluations of ICFR. Since management is an insider and the auditor is not, the two parties do not begin at the same point of knowledge when designing the necessary tests of operating effectiveness. The key point is that the difference between management and the auditor in their respective approaches to testing operating effectiveness will be much less if there is convergence on the decisions addressed through the eight risk assessment considerations. Thus, a well-documented management assessment maximizes audit cost-effectiveness. The documentation must include supporting rationale for management’s decisions about the critical risks and key controls. The good news is that much of this “rationale documentation” is a one-time investment, assuming no significant changes in business processes and the internal control structure.

The above dialogue between management and the auditors helps to maximize the extent of reliance by the auditor on the work of others in supporting management’s assessment, provided that work is performed by objective and competent personnel. The extent of the auditor’s reliance on the work of others is a significant cost driver to the compliance process.

Some of the key lessons relating to executing the Section 404 compliance project are as follows:

- As early as possible in the process, assess the entity-level controls and general IT controls. Plan on making fraud explicit in the assessment process.
- Inventory the company’s current controls documentation, and use process maps or other documentation to provide the most effective “walkthrough” of the critical processes. Based on the risk assessment, identify and document the key controls, i.e., the controls on which management relies for purposes of the Section 404 assessment. Note that the number of key controls is the most significant cost driver of the entire assessment process.
- Consider the risks of misstatement and control failure when defining the test plan. Use the risk assessment to define the “failure conditions” and articulate testing documentation protocols. Vary testing scopes according to frequency of the control, use appropriate sample sizes to obtain a reasonable level of assurance, use
competent and objective evaluators, and conduct refresh testing updates close to year-end when performing tests as of a preliminary date.

– The test plan might consider the use of self-assessment by control owners, or process owners or managers with no direct control responsibility, in low risk areas to self-assess the controls for which they are responsible and communicate the results to management. While self-assessments may be completed for all of the company’s key controls, i.e., those controls that are especially critical to the mitigation of risk, such controls normally require independent testing.

– The test plan should consider the monitoring activities taking place at two levels – the entity level and the process level. Management puts in place entity-level monitoring and analytics that provide direct evidence of control performance at the process level. Process owners put in place monitoring approaches through their direct supervisory activities and metrics on process performance. Monitoring is evaluated in terms of its precision in (1) determining that the key controls are operating effectively and (2) identifying material errors and/or omissions not detected by the underlying control processes.

– The test plan should consider independent direct tests of controls performed at both the entity level and at the process level. Tests at the process level include tests of pervasive process controls and information process controls. Periodic testing of key controls also evaluates the quality of self-assessment and monitoring processes.

• Consider timely the nature and extent of remediation requirements. Begin the evaluation process and tackle significant design deficiencies as soon as practicable. Thoughtfully remediate operating deficiencies in sufficient time to permit retesting of remediated controls.

• Management may document its overall strategy in a comprehensive memorandum that establishes the evaluation approach, the evaluation procedures, the basis for management’s conclusions about the effectiveness of controls related to the financial reporting elements and the entity-level and other pervasive elements that are important to management’s assessment of ICFR. If management determines the evidential matter within the company’s books and records is sufficient to provide reasonable support for its assessment, it may determine that it is not necessary to separately maintain copies of the evidence it evaluates.

Resources are often a challenge with Section 404 compliance, particularly in the first year. To address that issue, internal audit provides management a potential source of resources for purposes of complying with Section 404 of Sarbanes-Oxley. The COSO Framework points out that separate evaluations conducted by internal audit are a form of monitoring. Internal audit can play an important role in documenting internal controls, testing internal controls and providing input to management with respect to concluding on design and operating effectiveness.

**Japan**

Japanese companies have taken a number of measures to mitigate the costs of complying with the SOX requirements. Such measures include but are not limited to the following:

• **Reliance of external auditors on the testing performed by companies** – Over 60 percent of the 175 companies surveyed noted that their external auditors are relying on the testing of process-level controls conducted by the companies, while only a quarter said that no such reliance is made by their external auditors.
We note that whether external auditors can rely on the testing performed by companies depends on such factors as the quality of controls documentation, the extent to which controls are independently tested by internal auditors and the policies of external auditors in performing these audits. Making an effort to increase the external auditor reliance on the testing performed by companies would be beneficial for companies in two respects. First, it should contribute to improving the efficiency of the external audit. Second, it should also raise the quality level of both internal controls and internal audit.

- **Use of control self-assessment** – The survey revealed that more than 70 percent of the surveyed companies have introduced control self-assessment in one way or another. Controls are said to be self-assessed when they are tested not by independently positioned internal auditors but by control owner departments.

  We note that control self-assessment is advantageous not only because it makes it possible to allocate the control testing workload more evenly across the company but also because it can keep the process owners committed to maintaining and improving internal controls.

- **Exclude certain business locations from the scope of testing** – Following the revision of “Standards for Management Assessment and Audit concerning Internal Control Over Financial Reporting” issued by the Financial Services Agency of Japan in 2011, companies are now allowed to exclude a business location (such as a branch, a division or a subsidiary) from the scope of the testing of process-level controls, provided that the controls at that location were tested to be effective in the previous year and that no significant changes in the design of the controls have occurred since they were last tested.

  About 30 percent of the surveyed companies are taking advantage of this provision, while about 60 percent of the companies are not. We note that further rationalization of controls testing can be achieved by focusing on those business locations where the possibility of control failure is relatively high.

- **Relying on the control operating effectiveness test results of the previous year** – Similar to excluding certain business locations from the scope of testing, as noted above, the revised “Standards for Management Assessment and Audit” allows companies to rely on the operating effectiveness test results from the previous year for process-level controls, thereby making it possible for them to focus their testing effort on controls with greater importance or with a greater possibility of failure. Specifically, companies can choose not to test process-level controls for operating effectiveness provided that the controls were tested to be effective in design and operation in the previous year and that no significant changes in the design of the controls have taken place since they were last tested, except for those controls that are considered to be of material importance in ensuring the reliability of financial reporting.

  The survey results show that nearly 40 percent of the surveyed companies are relying on the operating effectiveness test results from the previous year for some controls, while about half the companies are testing all the process-level controls for operating effectiveness every year.
VII. SOX COMPLIANCE COSTS

United States and Japan

Protiviti asked 175 Japanese companies and almost 600 U.S. companies about how they weigh the benefits of complying with the SOX requirements relative to the costs. Their responses are summarized in the following graph:

While two-thirds of the Japanese companies think that the costs associated with SOX compliance exceed the benefits, 17 percent of the companies see net benefits from complying with the SOX requirements. These results compare with 31 percent of the U.S. companies surveyed by Protiviti in 2012 indicating that the benefits of SOX compliance exceed the costs and 50 percent who saw the costs in excess of the benefits.

Commentary: A larger proportion of the U.S. companies see the benefits that more than offset the costs because of the length of time they have complied with SOX and the maturity of the compliance process. During 10 years of SOX compliance, they have implemented measures to improve the efficiency of internal controls and the control assessment methodology and have proactively applied the SOX knowledge and experience to broader operations to bring about improvement in the efficiency and effectiveness of business processes.

In the United States, a 2012 Protiviti survey\(^\text{10}\) reported that a strong majority of large organizations leverage their SOX compliance efforts to drive continuous improvement in business processes that affect financial reporting, and a significant majority of organizations that are beyond their fourth year of compliance do so. Many large companies also are at or near the end of their efforts to improve the maturity of their Sarbanes-Oxley compliance processes.

After declining for several years, the 2013 Protiviti survey\(^\text{11}\) noted that U.S. SOX compliance costs were on the rise for many companies, and appear to be outpacing the rate of inflation in most companies; moreover, external audit fees are rising, as well. Specifically:


• Well over one-third of U.S. companies (38 percent) reported a year-over-year increase in SOX costs (2012 vs. 2011). And, as expected, the numbers are higher (52 percent) for the largest companies (e.g., large accelerated filers).

• For 87 percent of the companies reporting increased costs, the increase was greater than the rate of inflation (i.e., 5% or more), and for 42 percent of organizations, the increase was 15 percent or greater.

• For 75 percent of the organizations whose external audit fees rose, the increase was greater than the rate of inflation, and for half it was more than 10 percent.

The upward pressure on SOX compliance costs is likely due to recent PCAOB guidance that is directing external auditors to increase the thoroughness of their internal control reviews. This is increasing the demands auditors place on companies in providing evidence supporting their assertions regarding the effectiveness of ICFR.

Also, there is a general trend seen throughout the survey findings showing that U.S. organizations may be deriving fewer benefits and value from their SOX compliance processes than in previous years. This is likely a result of the increased maturity of their control structure and compliance process.

The majority of Japanese companies believe that the cost of complying with SOX regulations exceeds the benefits. Whether Japanese companies can reap further benefits from the SOX compliance appears to hinge on the extent to which they can utilize the SOX knowledge and experience in areas other than financial reporting to bring about improvement in their broader operations.
About SAC
Established in April 2013 as a statutory body of the Singapore government, the Singapore Accountancy Commission (SAC) is the lead agency in spearheading the development of the accountancy sector in Singapore.

The SAC’s Vision is for Singapore to be the Leading Global Accountancy Hub. This will be achieved through developing for Singapore a vibrant accountancy sector that enables the economy to grow, businesses to thrive and talent to flourish. In fulfilling this mission, the SAC seeks to uphold the values of being relevant, insightful, collaborative and advocative.

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, and has served more than 40 percent of FORTUNE 1000® and FORTUNE Global 500® companies. Protiviti and its independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. The firm also works 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.

Principal Contributors:

Protiviti
James DeLoach	Tracy Cui
Managing Director	Managing Director
Houston, USA	Beijing, China
Robert B. Hirth Jr.	Sidney Lim
Managing Director	Managing Director
(concurrently Chairman of COSO)
San Francisco, USA	Singapore

Yasumi Taniguchi	Ann Koh
Managing Director	Director
Tokyo, Japan	Singapore

Singapore Accountancy Commission
Uantchern Loh
Chief Executive

Violet Koh
Associate Director