



The MacLellan Group

Merchant Banking, Technology and Market Assessment Since 1992
8324 Delgany Avenue Playa del Rey, California 90293 USA
Tel: 310-301-7728 e-mail: maclellangroup@cs.com www.maclellangroup.com

By: Mr. Douglas C. MacLellan

July 17, 2006

SOX & Small-Cap Company Compliance

Sarbanes-Oxley: SOX represents the most significant change to federal securities laws since the 1930's. SOX was intended to provide protections for investors and to boost public confidence in the U.S. financial system. SOX covers issues such as establishing a public company accounting oversight board, auditor independence, corporate responsibility and enhanced financial disclosure.

A Non-Accelerated Filer: is a company that has under \$75 million in public float and makes its SEC filings under the small business issuer rules. These Non-Accelerated filers are all either "Small-cap" & "Micro-cap" companies, which still must go through the process of SOX 404 compliance, certification and attestation. Basically, all Large Accelerated and Accelerated filers must have already complied with SOX 404 fully as of December 31, 2005. It is now only the Non-Accelerated filers that still have this challenge in front of them. Yet, this group of companies is the largest in terms of number of all U.S. publicly listed companies. Approximately 52.6 percent of all public companies fit into the micro-cap definition, and an additional approximately 25.9 percent of all public companies fit into the small-cap definition. This means that approximately 78.5 percent of all U.S. public companies are subject to the full compliance of SOX 404.

SOX 404 Is Here To Stay: Although the SEC recently extended the SOX 404 compliance date for non-accelerated filers & foreign private issuers and they have indicated that they will be issuing new slightly slimmed-down guidance for Small-cap and Micro-cap companies. Yet, do not expect the compliance date to be delayed again. This means non-accelerated filers (with calendar year end's), will need to be fully SOX compliant no later than December 31, 2007. Due to the implementation, testing and attestation phases of the SOX compliance process, companies need to start immediately if they intend to meet this deadline.

The Costs: The costs of such compliance have proved to be high, especially on small-cap companies. Recent studies have shown average compliance costs for such companies to be as high as 2.5 percent of revenues. Regardless of various views on SOX, it is here to stay and compliance is mandatory for all U.S. listed public companies. Based upon various discussions with multiple accounting firms and 404 compliance consultants any small-cap company should anticipate spending at least \$175,000 over 12-18 months. Micro-cap companies should anticipate spending at least US\$75,000 over a 12-18 month period. At the very minimum, companies should anticipate hiring at least one full-time employee as the SOX 404 control person. Each year SOX consultants will have to re-affirm a companies SOX 404 compliance position and any acquisitions made by companies will have to conform to the SOX 404 standards. Lastly, anticipate that a company's auditors will charge for their initial and ongoing annual certification and attestation that is anticipated to raise a company's existing accounting fees by as much as 100 percent during the initial compliance year and as much as 30% in the following years, excluding any acquisitions.

What To Do Next: If your company hasn't already started their SOX 404 compliance work then consider contacting the MacLellan Group, which has developed relationships with various SOX 404 consulting firms and software companies and is capable of providing companies with various recommendations on meeting their SOX 404 compliance needs.

Mr. Douglas MacLellan holds significant expertise in developing and financing businesses in emerging markets and industries, particularly in the pharmaceutical telecommunications, software and media industries. Over the past fifteen years, Mr. MacLellan has helped to develop and finance businesses in Bulgaria, Cambodia, Canada, Chile, China, Hungary, India, Korea, Madagascar, Russia and the United States. Mr. MacLellan is currently a member of the Board of Directors and Chairman of the audit committees of two publicly listed companies.

SOX General Overview

A View From The Beginning: It came as a result of the large corporate financial scandals involving: Enron, WorldCom, Global Crossing, Tyco, HealthSouth, and Arthur Andersen. The Sarbanes-Oxley Act of 2002 (Pub. L. No. 107-204, 116 Stat. 745, also known as the Public Company Accounting Reform and Investor Protection Act of 2002 ("**SOX**"), sponsored by Senator Paul Sarbanes (D-Md.) and Representative Michael G. Oxley (R-Oh.), was approved by the House by a vote of 423-3 and by the Senate 99-0.



Before the signing ceremony of the Sarbanes-Oxley Act, President George W. Bush meets with Senator Paul Sarbanes, Secretary of Labor Elaine Chao and other dignitaries in the Blue Room at the White House, July 30, 2002.

The Sarbanes-Oxley Act's 11 Major Provisions: SOX represents the most significant change to federal securities laws since the 1930's. SOX was intended to provide protections for investors and to boost public confidence in the U.S. financial system. The Act covers issues such as establishing a public company accounting oversight board, auditor independence, corporate responsibility and enhanced financial disclosure. The Act contains 11 titles, or sections, noted below that range from additional Corporate Board responsibilities to criminal penalties, and requires the Securities and Exchange Commission ("**SEC**") to implement rulings on requirements to comply with the new law.

1. **Certification of financial reports by chief executive officers and chief financial officers;**
2. **Ban on personal loans to any Executive Officer and Director;**
3. **Accelerated reporting of trades by insiders;**
4. **Prohibition on insider trades during pension fund blackout periods;**
5. **Public reporting of CEO and CFO compensation and profits;**
6. **Additional disclosure;**
7. **Auditor independence, including outright bans on certain types of work and pre-certification by the company's Audit Committee of all other non-audit work;**
8. **Criminal and civil penalties for violations of securities law;**
9. **Significantly longer jail sentences and larger fines for corporate executives who knowingly and willfully misstate financial statements;**
10. **Prohibition on audit firms providing extra "value-added" services to their clients including actuarial services, legal and extra services (such as consulting) unrelated to their audit work; and**
11. **A requirement that publicly traded companies furnish independent annual audit reports on the existence and condition (i.e., reliability) of internal controls as they relate to financial reporting.**

Value & Costs of SOX

Views On The Value Of This Legislation: Some believe the legislation was necessary, others believe that the Sarbanes-Oxley Act does more economic damage than it prevents and yet others observe how essentially modest the Act is compared to the heavy rhetoric accompanying it. **Management of publicly listed companies face a daunting challenge in documenting all critical operational controls, assessing the effectiveness of these controls, and subjecting the assessment report to the scrutiny of independent auditors.** The costs of such

compliance have proved to be high, especially on small cap companies. Recent studies have shown average compliance costs for such companies to be as high as 2.5 percent of revenues. **Regardless of various views on SOX, it is here to stay and compliance is mandatory for all U.S. listed public companies.**

Cost Of Implementing SOX: There is considerable debate over the specific requirements of the Sarbanes-Oxley act, as written. Some people in the business community have acknowledged that, as John Thain, CEO of the New York Stock Exchange states, "There is no question that, broadly speaking, Sarbanes-Oxley was necessary". However, the cost of implementing the new requirements has led some to widespread questioning of how effective or necessary the specific provisions of the law truly are. The auditing industry had lobbied for this requirement for decades. Ironically, the collapse of one of its members in the scandals (Arthur Andersen) finally earned the industry this lucrative new line of work. **For U.S. publicly listed companies, a key concern is the cost of updating information systems to comply with the control and reporting requirements. Systems that provide document management, access to financial data, or long-term storage of information must now provide auditing capabilities. In most cases this requires significant changes to, or even complete replacement of, existing systems that were designed without the newly required level of auditing details.**

Accelerated, Large Accelerated & Non-Accelerated Filers

A Non-Accelerated Filer ("Issuer", "Registrant" and or "Company") is a company that has under \$75 million in "Public Float" and makes its SEC filings under the small business issuer rules. Public Float is defined as, the portion of a company's outstanding shares that is in the hands of public investors, as opposed to company officers, directors, or controlling-interest investors. **These Non-Accelerated filers are all either "Small-cap" & "Micro-cap companies, which still must go through the process of SOX 404 compliance, certification and attestation. Basically, all Large Accelerated and Accelerated filers must have already complied with SOX 404 fully as of December 31, 2005. It is now only the Non-Accelerated filers that still have this challenge in front of them. Yet, this group of companies is the largest in terms of number of all U.S. publicly listed companies.** In 2002, the SEC adopted rules that subjected accelerated filers companies with \$75 million or more in public float to accelerated deadlines for their annual and quarterly reports. The accelerated deadlines were to be phased in gradually over a three-year period; however, in 2004 the SEC postponed the final phase-in of the accelerated deadlines. On December 14, 2005, the SEC adopted amendments to these periodic report filing deadlines, and, in doing so, amended the definition of an accelerated filer. The new definitions are as follows, "**large accelerated filers**" include companies with a public float of \$700 million or more. While, "**accelerated filers**" has been redefined as companies that have at least \$75 million, but less than \$700 million, in public float. The amendments also modified the exit requirements out of accelerated filer status by permitting an accelerated filer whose public float has dropped below \$50 million to file an annual report on a non-accelerated basis for the same fiscal year that the determination of public float is made. The amendments permit a large accelerated filer to exit out of large accelerated filer status once its public float has dropped below \$500 million.

The Size of the Small-Cap & Micro-Cap Marketplace

SOX & Small-Cap Companies: A similar clash of attitudes colors the recent debate over the extent to which SOX should apply to small public companies. The most visible argument is that small companies should not have to shoulder the same compliance burdens as large companies do, simply because they can't afford to. But that premise is being challenged by studies, derided by a number of commentators and viewed with public skepticism even by some SEC Commissioners. It assumes that were money no object, small and large companies should be regulated the same. If that assumption is true, then any argument for relaxed compliance that hinges on expense is vulnerable. Cost seldom satisfies as a reason for not doing something that ought otherwise be done. However, it is wrong to assume that the main difference between small and large companies is how much money they have. Large and small companies play very different roles in the national economy and in the minds of investors. The very large companies really are different than their smaller firms, and not just because they have more money.

Defining the Small Public Company Market: It is helpful to understand what the SEC means by "smaller public company." The SEC has proposed two classifications. The first is "micro-cap companies," which consists of those companies whose outstanding common stock, in the aggregate, comprises the lowest 1 percent of total U.S. equity market capitalization, and the second is "small-cap companies," which consist of those companies whose outstanding common stock, in the aggregate, comprises the next lowest 5 percent of total U.S. equity market capitalization. This clearly doesn't sound like much. **Yet, according to the SEC figures, approximately 52.6 percent of all public companies fit into the micro-cap definition, and an additional approximately 25.9 percent of all public companies fit into the small-cap definition; this means that approximately 78.5 percent of all U.S. public companies are now going to have to be fully compliant with SOX 404. It is estimated that over 7,200 Small-Cap and Micro-Cap companies still need to comply to SOX 404.**

SOX Compliance Deadlines

Clarifying the SEC's Latest Section 404 Deadlines: If you were wondering whether maybe, just maybe, the SOX 404 requirements would somehow vanish for small business filers, wonder no more. Although the SEC recently extended the SOX 404 compliance date for non-accelerated filers and foreign private issuers, do not expect the compliance date to be delayed again. In a May 17, 2006 press release on Section 404, the SEC stated that there will be a new short postponement of the effective date for the rules implementing Section 404 for non-accelerated filers, this statement noted that all filers will nonetheless be required to comply with the Section 404(a) management assessment for fiscal years beginning on or after December 16, 2006. Many executives were confused because under the prior deadline, emanating from SEC Release 33-8618 from September 2005, non-accelerated filers were not required to comply with the rules under 404 until the first fiscal year ending on or after July 15, 2007. This means non-accelerated filers for companies that have between a December 16th through a December 31st financial year-end, will need to be fully compliant on SOX 404 internal controls over financial reporting no later than December 31, 2007. More importantly, In the event that a company has between a January 1 through a December 15th year-end, then the deadline is on the date that the company's year-end occurs during 2008.

The SEC Deadline Is Barely Manageable Given The Work That Has To Be Done

The following is an overview, for December 31st filers, of the timing to comply with SOX 404, the following is an example of the 5 major steps that must be followed in order to meet the compliance deadline.

1. Working back from a December 31st 2007 deadline, it is highly likely that any public company's auditors will want to review and attest to the preceding financial period (i.e.: period ending September 30, 2006). This financial period begins July, 1, 2007. Thus, a fully functioning SOX 404 compliance regime must be fully in place prior to July 1, 2007.
2. The pre-attestation SOX testing and validation process should last a minimum of one quarter, which then takes the process back to April 1, 2007.
3. Before this, the company will be documenting controls and completing assessment effectiveness, taking at least 90 days which brings the process back to December 31, 2006.
4. Prior to this phase, the company will be completing the document process and risk assessment phase which will take at least 90 days, which brings the process back to September 30, 2006.
5. The process then begins with the prioritization of the SOX 404 process for a specific company that can again take up to 90 days to complete, which takes the process back to June 30, 2006.

Given the above noted schedule, all small-cap and micro-cap companies should have already commenced their SOX certification process with the help of knowledgeable SOX compliance consultants. Yet, if your company is one of the few issuers with a non-December 31 year-end, then you'll have a bit more time to get started on your 404 compliance work.

New SEC Guidance On The Implementation of SOX 404

SEC Indicates A More Flexible View on the Implementation of SOX 404: On July 11, 2006 the SEC, published a Concept Release as a prelude to its forthcoming: Guidance for Management in Assessing a Company's internal Controls for Financial Reporting. This Concept Release indicates that the totality of internal controls related to 404 may be slightly reduced for Small-cap and Micro-cap companies. **Regardless of the ultimate language of this guidance, the breadth and depth of the SOX 404 process will continue to be significant. Companies should be already in-process with the implementing their SOX 404 compliance solutions now, not later.**

Overview of SOX Section 404

Section 404, 409 and 303: Issuers will be required to publish a statement in their annual reports that management of the issuer is responsible for establishing and maintaining an adequate internal control structure and procedures for financial reporting. This statement shall also assess the effectiveness of such internal controls and procedures. Issuers must have a consistent, defined and documented process for all transactions. **Issuers must have credit**

policies mapped to their overall corporate strategy, regardless of the number of operating divisions, subsidiary operations or foreign locations. Lastly, issuers are required to report quarterly.

SOX Section 404: The centerpiece of SOX 404 compliance is Section 404, which requires corporations to adopt and continually assess the effectiveness of internal accounting controls, and requires their auditors to report on management's assessments and opine on the effectiveness of the controls themselves. The 404 assessments and the auditor opinions have generated a lot of work for corporations, their advisors and accounting firms. Section 404's requirements are tailor-made for large corporations. For one thing, the only exact standard for internal controls was designed for large businesses. It was then and still is the 1992 Internal Control Integrated Framework developed by the Committee of Sponsoring Organizations of the Treadway Committee ("**COSO**"), a private group sponsored by several major accounting and management organizations. **The SEC specifically identified the COSO Framework as the de facto standard for internal controls in promulgating its first round of rules under 404.** SOX 404 requires a security management process to protect against attempted or successful unauthorized access and use with system operations. SOX 404 also involves security management for disclosure, modification, or interference with system operations. The SEC ruled that the criteria on which management's evaluation is based must be derived from "a suitable, recognized control framework 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 the final rules that the COSO Internal Control – Integrated Framework satisfied this requirement of SOX 404.

SOX Top-down Overview: Item number 2 from the below listed summary is by far the most time consumptive part of the process and requires a considerable amount of flowcharting and written descriptions of the current state of internal controls in the various components of the organization. This section also includes actual testing of many processes. However, this section cannot be approached in a logical or efficient manner until a thorough assessment process has been completed. **Therefore unless the first step is correctly performed the results will be flawed and would not satisfy the accounting firm that certifies your financial statements.** A very high level summary of the 404 certification process is as follows:

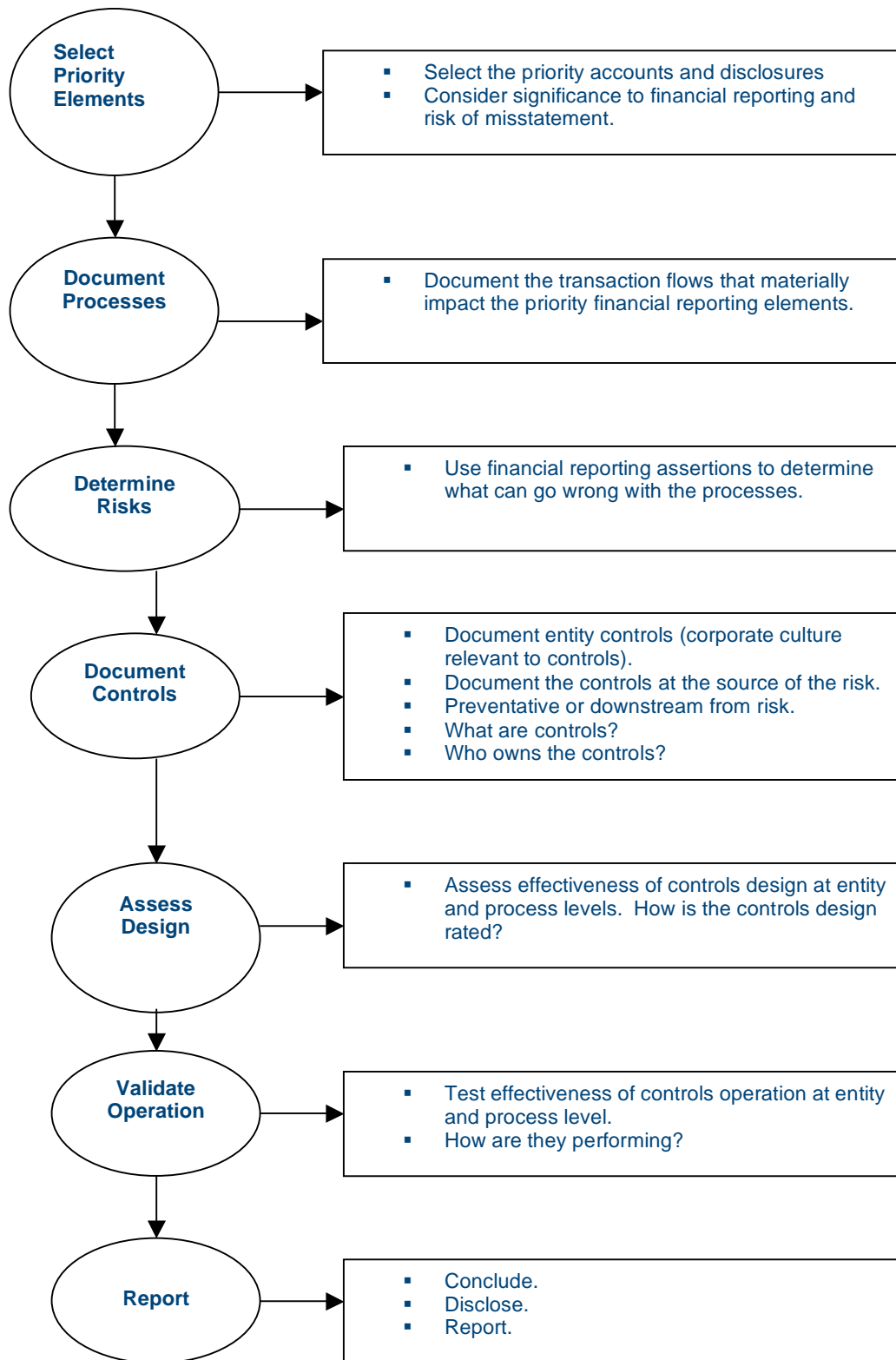
- 1) **Assess current state and identify relevant processes;**
- 2) **Document and evaluate critical processes and controls;**
- 3) **Design solutions for control gaps;**
- 4) **Implement solutions for control gaps;**
- 5) **Test that solutions are in effect and working; and**
- 6) **Report on all of the above.**

SOX 404 compliance Process

SOX 404 Compliance: Issuers are required to disclose to the public, on a rapid and current basis, information on material changes in their financial condition or operations. These disclosures must be presented in terms that are easy to understand, supported by trend and qualitative information with graphic presentations as appropriate. Businesses must be able to make real-time assessments of their customer base and report the material changes to the SEC within four business days in an 8K report if there are issues impacting and/or impairing the quality of an asset such as accounts receivable ("**A/R**"). Section 404 requires management to file an internal control report with the annual report. The internal control report must articulate the following:

1. **Management's responsibilities to establish and maintain adequate internal controls and procedures for financial reporting;**
2. **Management's conclusions as to the effectiveness of these internal controls and procedures for financial reporting based on management's evaluation of them, at year-end; and**
3. **The report must also state that the company's public accountant has attested to and reported on management's evaluation of internal controls over financial reporting.**

Section 404 Certification Process Chart



PCAOB Audit Standards Process

Working With The PCAOB: Under both **Section 302** and **Section 404**, Congress directed the SEC to promulgate regulations enforcing these provisions. **In addition, outside auditors for companies must, for the first time, attest to managers' internal control assessment. This presents new challenges to businesses, specifically, documentation of control procedures related to information technology. Public Company Accounting Oversight Board (PCAOB) has issued guidelines on how auditors should provide their attestations. Yet, the SEC indicated in their May 17, 2006 press release that they would be, in the future, issuing a Concept Release on various changes to Section 404 (a) and (b) that would give additional guidance on the appropriate roll of outside audits in connection with management assessment and auditor attestation. This Guidance is anticipated to become available during the 3rd quarter of 2006.**

Auditing Standard No. 2' of PCAOB: Part of the SEC's program to make compliance with Section 404 more efficient is to work closely with the PCAOB in its effort to improve auditors' implementation of PCAOB requirements for audits of internal control over financial reporting. The PCAOB's program, announced the same day as the SEC's, includes amending Auditing Standard No. 2 and reinforcing auditor efficiency through PCAOB inspections. The SEC staff will examine whether the PCAOB's 2006 inspections have been effective in encouraging auditor efficiency. The PCAOB's amendment to Auditing standard No. 2 will be intended to ensure that auditors focus on areas that pose a higher risk of fraud or material error. The project will include revisiting the auditor's role in evaluating management's assessment process. It will consider clarifications or additional guidance regarding the following elements of the standard on audits of internal control over financial reporting: the definitions of significant deficiency and material weakness in internal control, materiality and scoping decisions, integrating the internal-control and financial-statement audits, applying prior year's experience, using work by other parties, and evaluating potential deficiencies. The PCAOB intends to establish an effective date for the amendment that minimizes disruption to audits that are in process. The PCAOB's program also includes developing implementation guidance for auditors of small companies or facilitating the development of that guidance. The PCAOB will continue to hold forums on auditing in the small-business environment for financial officers, directors, and auditors of smaller public companies. **The Auditing Standard No. 2' of PCAOB has the following key requirements:**

1. **The design of controls relevant assertions related to all significant accounts and disclosures in financial statements;**
2. **Information about how significant transactions are initiated, authorized, supported, processed and reported;**
3. **Enough information about the flow of transactions to identify where material misstatements due to error or fraud could occur;**
4. **Controls designed to prevent or detect fraud, including who performs the controls and the regulated segregation of duties;**
5. **Controls over the period-end financial reporting process;**
6. **Controls over safeguarding of assets; and**
7. **The results of management's testing and evaluation.**

Revisions to Auditing Standard No. 2. The PCAOB announced May 16, 2006, a four-point plan to improve auditors' implementation of SOX 404 that includes: Amending Auditing Standard No. 2. AS2, "An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements," establishes the professional standards for auditors when conducting an audit of internal control over financial reporting. The PCAOB intends to maintain the general principles of AS2, but plans to consider amendments that would ensure that auditors' primary focus is on areas involving higher risk of fraud or material error and that incorporate key concepts contained in the May guidance (designed to reinforce the PCAOB's expectations of efficiency in the audit process). The PCAOB also plans to "revisit and clarify the auditor's role, if any, with respect to evaluation of the process that a company uses to reach its own conclusion about the effectiveness of company controls." (Emphasis added.) Additional amendments to AS2 under consideration include:

1. **Clarifying the definitions of "significant deficiency" and "material weakness";**
2. **Reconsidering the "strong indicators of a material weakness" to allow the exercise of more judgment;**
3. **Guiding auditors to increase their use of the work of others where appropriate;**
4. **Clarifying materiality and scoping decisions;**
5. **Emphasizing the integration of the audit of internal control with the audit of the financial statements; and**

6. **Allowing for and promoting auditors' use of experience gained in previous years' audits to focus and make most efficient the work in subsequent years.**

The PCAOB confirmed that the effective date for any amendments to AS2 would minimize unnecessary disruption to ongoing audits. To that end, **the PCAOB plans to develop or facilitate development of "implementation guidance" and to facilitate opportunities for training of auditors of smaller public companies. The PCAOB indicated that they intend to hold eight forums during 2006 for auditors, directors and financial officers of smaller public companies, designed to provide general education and to allow the PCAOB to monitor reaction to internal control implementation changes.**

SOX 404 Internal Controls Requirements

Internal Controls: Under SOX, two separate certification sections came into effect, one civil (**Section 302**) and the other criminal (**Section 906**). **Section 302 of the Act mandates a set of internal procedures designed to ensure accurate financial disclosure.** The signing officers must certify that they are, "responsible for establishing and maintaining internal controls" and "have designed such internal controls to ensure that material information relating to the company and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared." **The officers must "have evaluated the effectiveness of the company's internal controls as of a date within 90 days prior to the report" and "have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date."** As important, under Section 404, management is required to produce an "internal control report" as part of each annual Exchange Act report. **The report must affirm "the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting"**. The report must also "contain an assessment, as of the end of the most recent fiscal year of the Company, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting." To do this, companies are generally adopting an internal control framework such as that described in COSO.

Internal Controls Over Financial Reporting SOX 404 defines internal controls over financial reporting as, "controls that pertain to the preparation of financial statements for external purposes that are fairly presented in conformity with generally accepted accounting principles as addressed by the Codification of Statements on Auditing Standards 319". The actual Auditing Standards 319 defines internal controls as follows: **A process effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: Reliability of financial reporting, effectiveness and efficiency of operations and Compliance with applicable laws and regulations.** The Auditing Standards 319 further provides that internal controls over financial reporting consist of the following five interrelated components:

- 1) **Control Environment: Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure;**
- 2) **Risk Assessment: This component is the entity's identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks should be managed;**
- 3) **Control Activities: Includes the policies and procedures that help ensure that management directives are carried out;**
- 4) **Information and Communication: This component consists of procedures and systems that support identification, capture and exchange of information in a form and time frame that enable people to carry out their responsibilities; and**
- 5) **Monitoring: Consists of the processes that assess the quality of internal control performance over time.**

The COSO Framework

The COSO Framework: The COSO Framework is a treatise on the theory and practice of principle-based internal accounting controls, and as a theory it ought to be applicable to all companies. But as a framework, it works only for large enterprises because it assumes a management that is procedure-based. The idea behind the COSO Framework is to subject a company's internal procedures to testing by persons outside of these procedures. The framework thus assumes divisions of responsibility and systems of checks and balances within the company. That is how a large enterprise must be run, and the framework has evolved over the past decade as large corporations have adopted it, to the point where, for a large company, SOX compliance does not present much of an added burden. The COSO framework has three dimensions :

1. The type of controls (operations, financial reporting, compliance);
2. The organizational dimension (enterprise, business unit, activity/process); and
3. The five components of effective internal control (control environment, risk assessment, control activities, information and monitoring).

Using the COSO framework, a company must address all five internal control components at the appropriate levels (enterprise, business unit) and the activity/process levels that relate to financial reporting. Companies must also consider writing higher-level information security policies that can be applied across the board and cover as many regulations as possible. **Most regulations have similar requirements and there's certainly no need for duplication. This will likely save a significant amount of time and effort when it comes to managing security policies long-term. Keeping information security as simple and practical as possible is critical.**

Information Technology & SOX

IT Controls, IT Audit & SOX: The financial reporting processes of most organizations are driven by IT systems. Few companies manage their data manually and most companies rely on electronic management of data, documents, and key operational processes. Therefore, it is apparent that IT plays a vital role in internal control. **As PCAOB's "Auditing Standard 2" states: "The nature and characteristics of a company's use of information technology in its information system affect the company's internal control over financial reporting." Systems such as Enterprise Resource Planning ("ERP") are deeply integrated in the initiating, authorizing, processing, and reporting of financial data.** As such, they are inextricably linked to the overall financial reporting process and need to be assessed, along with other important process for compliance with SOX. So, although SOX signals a fundamental change in business operations and financial reporting, and places responsibility in corporate financial reporting on the chief executive officer ("**CEO**") and chief financial officer ("**CFO**"), the chief information officer ("**CIO**") plays a significant role in the signoff of financial statements. **Many small-cap companies don't have a CIO, during the SOX compliance process these companies can outsource this function to professional SOX compliance consultants.**

Section 404 Executive, Board and Committee Roles & Responsibility

Roles	Responsibilities
Board of Directors	<ul style="list-style-type: none"> ▪ Hire external auditors & review results of audits ▪ Financial expertise
Audit Committee	<ul style="list-style-type: none"> ▪ Continued expansion of their role in the corporate reporting framework including direct responsibility for overseeing the external audit process, pre-approval of all audit and non-audit services, revised rules regarding independence and financial expertise and monitoring, receiving and resolving complaints regarding corporate reporting and audit issues
CEO & CFO	<ul style="list-style-type: none"> ▪ Setting <i>tone at the top</i> ▪ Approve policies ▪ Sign management attestation letters
CIO	<ul style="list-style-type: none"> ▪ Develop IT policies ▪ Develop an internal control compliance plan and integrate into the organization's overall SOX compliance plan ▪ Review results of testing and resolve issues ▪ May sign management attestation letters
IT Management	<ul style="list-style-type: none"> ▪ Define required internal controls ▪ Develop, maintain, educate and make available to staff: documented processes and procedures ▪ Test internal controls and correct remediation

404 Reporting Requirements

Large-Cap Organizational 404 Reporting Requirements: The typical process that has been followed by the larger companies that have been required to comply with Section 404 generally followed one of the following approaches.

1. Those companies with fairly sophisticated internal audit departments hired consulting firms to manage the project with a lot of the low level work being actually performed by the internal auditors. The assessment process and the determination of review and testing parameters would be set by the outside firm in these instances. In the companies that used this approach a higher-level

financial executive from each of the entities in the company would be assigned as the liaison individual. This would typically be the head of internal auditing and the controller.

2. The very large companies with large, highly sophisticated internal audit departments would utilize outside consultants, but to a much lesser degree and would perform much more of the assessment and management of the process.

Small-Cap Organizational 404 Reporting Process: As Small-cap and Micro-cap businesses start the SOX 404 compliance process it will be more difficult, as many do not have internal audit department or multiple higher level financial personnel. **These companies they will have to rely much more heavily on outside SOX 404 consulting firms in order to assist them in perform most of the review process. However, it is important to note that executives within a company will have to spend a significant amount of time initially with the outside SOX compliance advisors, particularly during the assessment phase.** It is generally accepted that a broad range of information security controls are necessary; the most critical component being assuring the integrity of financial information. As with most security-related initiatives, these measures must be policy-driven in order to be effective. Every organization's security policy requirements are based on several variables, perhaps the most important of which is based on the outcome of a risk analysis or ongoing IT security audits. However, there are several security policies that most corporations will need in order to become SOX 404 compliant, regardless of their size, setup and business processes. **Formatting SOX compliance policies for maximum effectiveness may seem detailed and complex, but there is a simple template approach you can take when writing them. Once your compliance policies have been set, enforcing them is equally important. These policies include:**

1. **Access Controls:** Hardware/software controls regulating who has access to what financial-related information;
2. **Audit Trails:** Application, operating system, etc. logs that track who has accessed, modified or deleted financial information;
3. **Computer and Media Disposal:** Minimum requirements for ensuring financial-related information is wiped before hardware and media leave the company;
4. **Data Backup:** Specific backup requirements to ensure financial data is properly protected;
5. **Data Integrity Controls:** Hardware/software solutions to keep financial information from being inappropriately modified (i.e. IDS/IPS, rights management software, application controls to filter input and perform data validation, etc.);
6. **Data Retention:** Minimum requirements for holding onto critical financial data, especially supporting documentation, related communications, etc;
7. **Document Destruction:** Requirements and steps to be taken (or not taken) when destroying hard copy information;
8. **Information Classification:** Outlining how various types of financial information will be classified and protected based on level of sensitivity;
9. **Messaging Security:** Minimum requirements for protecting the transmission and storage of messages (e-mail and instant messaging) containing sensitive financial-related information;
10. **Security Assessments and audits:** How systems will be continuously tested and audited for security risks;
11. **System Authentication:** Hardware/software controls ensuring that users accessing financial information are who they say they are;
12. **System Monitoring:** Technologies and processes in place to detect and alert on financial information breaches;
13. **User Provisioning:** Specific requirements and processes for adding and removing users who will have access to financial information; and
14. **Wireless Networks:** Minimum security requirements for wireless systems connecting to corporate networks.

SOX Software Systems

Most organizations have implemented paper and MS Excel-based processes to document and test internal controls over financial reporting to comply with Section 404. Consequently, a large amount of time and effort is consumed in scheduling tests, manually testing the internal controls, identifying and tracking remediation, compiling and cataloging evidence, implementing change control and managing the entire process. In addition, most organizations lack a systematic and comprehensive approach to assessing IT controls that impact financial transactions. Testing of IT controls is often not integrated into the overall SOX compliance program. **Control activities are the policies, procedures and practices that are put into place to ensure the business objectives are achieved and risk mitigation strategies are carried out. IT controls include such things as system software control and security controls.**

The Positive View On Using Spreadsheets for SOX Compliance

Industry surveys indicate that the majority of companies impacted by SOX have elected so far to tackle SOX using a combination of word processing and spreadsheets, the "**low-tech solution**". The reasons for using these types of software tools include:

- 1. The company's external auditors and/or SOX project advisors like using Excel spreadsheets and often recommend they be used for SOX assessment work;**
- 2. There isn't enough time to properly evaluate and select a SOX software product;**
- 3. Choosing the spreadsheet option is inexpensive, as most companies already have licenses to use Excel or equivalent software;**
- 4. Most SOX participants are familiar with spreadsheet packages;**
- 5. SOX requirements are still evolving and the SEC and/or PCAOB may change the rules;**
- 6. Many of the vendors in the space are new and there will be a shakeout in the industry as some of the SOX software vendors will likely fail or will be absorbed by other software firms; and**
- 7. The use of spreadsheets that do not include critical data input fields and assessment features allow consultants and external auditors to hide major deficiencies in their technical SOX assessment work. (Note: This is only a positive for the consultant and/or external auditor charging 404 compliance fees, not the CEOs and CFOs certifying the company's representations to the SEC.)**

The Negative View On Using Spreadsheets for SOX Compliance

No Link Between Accounts, Risks and Controls: If having controls that actually do what is required is an objective, it is essential that the people responsible, and those that oversee them, are able to see the relationship between objectives, risks, the controls in place, and, ideally, the actual results being achieved. This fundamental continuous improvement prerequisite underpins the total quality movement and well known process analysis techniques like Six Sigma. Spreadsheets are not well equipped to display and continuously track that relationship.

Doesn't Foster Work Unit Ownership and Accountability: A key feature in many of the SOX software products on the market is the ability to assign "owners" of "sponsors" to control representations, processes, deficiency disclosures, control testing, verification of control testing, and other important elements. This functionality allows companies to efficiently "divide and conquer" by electronically assigning accountability for the many activities that must be done to support a SOX representation. While a very diluted form of accountability and role definition is possible using spreadsheets alone, it is not easy to accomplish.

Poor Security and Reliability: Audit Standard No. 2 requires that an IT general controls assessment be completed on all applications used to assess and monitor controls, including spreadsheet applications used for SOX assessments.

Doesn't Build Control Assessment Skills: Because of the time urgency and the heavy workload in round one many companies used outside consultants and/or project teams to complete the first full set of risk and control assessment documentation. This was often done using pre-populated assessment templates provided by the consultants. Although this approach got the job done it missed an opportunity, the opportunity to introduce the fundamentals of risk assessment to staff all across a company. **It is likely that the typical small-cap and certainly micro-cap company lacks executives with the background or capability to perform the analysis and some of these companies have executives who will not be capable of absorbing the process and performing proper assessments after the initial assessments are performed.** Spreadsheets, especially those with "canned" questions, do not allow users to see the one to many relationships between specific risks, the controls in use and the

resulting residual risk position and they don't foster work unit ownership and maintenance of the assessments. SOX can be used as training tool to teach a logic-based approach to risk assessment to lay a foundation to "embed" risk and control assessment across the organization.

Doesn't Allow Efficient Integration of Testing Done by Management and Internal and External Auditors: Once a company has completed the first full round of SOX control design assessment documentation the next step is to test that the "key controls" are in fact resulting in an acceptable error/exception rate. This testing work should be done in a way that CEOs and CFOs are able to see how much work has been done to support the organization's assessment and the representations they are personally making to the SEC in 10K and 10Q filings. The use of spreadsheets does not allow for effective integration and secure storage of testing work on the control assessment documentation. It also does not keep the costs of planning, scheduling and performing the required testing to the minimum amount possible.

Good SOX Compliance Software

What a SOX Software Solution Ideally Should Provide: First, it should include or be integrated with the functionality of an audit tool, imposing a COSO-oriented table structure on the company's financial accounts, transactions, risks and controls, assuring completeness and best practices in the eyes of the auditor. Second, recognizing that controls and effectiveness testing results are in reality managed as documents that must be secured, reviewed, revised and approved, the solution should include a document management repository supporting basic library services and a complete audit trail. SOX solutions built on an ECM platform can also offer enhanced capabilities such as collaboration and records management. Third, the ideal solution should provide workflow automation of the SOX compliance process itself: **risk assessment, documentation, effectiveness testing and reporting**, in order to streamline the effort and meet the deadline. As with the document management component, the goal should be maximum distribution of workload throughout the organization, while maintaining central control and management. **Fully featured SOX software packages are available on the market starting at approximately \$1,000 per user.** The features and benefits of a good SOX software package should have the following components:

1. **Flexible 404 control testing model. Typically a two-tiered approach, where key controls are subjected to formal assessment and testing and secondary control effectiveness are evaluated by surveying line management, reducing the overall number of controls requiring formal testing;**
2. **A single compliance repository for all control data including: all controls, documentation, test results, evidence and other artefacts are retained in one single repository managed in accordance with record retention obligations;**
3. **A risk based financial control management. Typically a top-down risk assessment model that ensures ongoing identification of high-risk controls and provides a means for focusing control testing efforts on high risk controls;**
4. **The automation of 404 control testing and assessment processes. Typically this would automatically notifies and prompts control owners of pending assessments and provides them with access to all needed collateral;**
5. **Real-time visibility over 404 compliance status, including flexible, real-time reporting, giving immediate insight into control effectiveness status and revealing compliance hot spots;**
6. **Remediation management of critical failures, where ineffective controls automatically subjected to the remediation management process;**
7. **Escalation of 404 control assessment and test failures, where failed or overdue control tests are automatically raised to the attention of control owners and management;**
8. **Support of 404 audit assurance process, that would include incorporating two levels of assurance testing, for internal and external audit teams to assess the effectiveness of the control environment;**
9. **Facilitates Quarterly Certification, where information captured relating to 404 compliance flows through to support quarterly SOX 302 certification which can also be completely manned by the software; and**
10. **Control Environment Changes, where changes to entity structures and control models with full historical retention.**

SOX and IT Controls

Simplifying the Situation: In all cases a company will need to manage multiple requests to enhance IT documentation, provide documentation in specific formats, change its operating procedures and endure testing by multiple parties. A company can avoid the costly task of reproducing documentation in multiple forms and formats and clearly link business units and their understanding and roles in SOX compliance by adhering to 4 basic rules:

Get Educated: Have a company's management hold a meeting with your public company accountants so they can provide insights into IT general controls. Make sure you're all on the same page. Be sure your team understands how SOX fits into the IT environment. **You should make sure that a specialized 404 IT consulting firm is involved from the beginning of the project and is updated and included in the review of business processes that rely on IT systems and infrastructure.** Be sure to leverage documentation you have in place. For example, many pharmaceutical and manufacturing companies already have to comply with federal regulations and many are ISO 9000 certified. It is important that IT departments leverage existing procedures, policies, and documentation in their SOX programs. Be sure you design your program to fit your business needs. Don't adapt what you do to fit a generic set of best practices. **Your IT SOX 404 program should be tailored to your business requirements.**

Hire Advisors that Understand Both IT Management and SOX 404. Many auditing firms are experts in accounting, auditing and SOX, but have never managed an IT department, but many companies require front-line expertise to determine what makes sense for the company. There is a significant amount of translation required to convert accounting practices into terms and actions that can be implemented in any IT solution. **The CIO or counterpart should be part of any company SOX steering committee.**

Modify Standardized Procedures. Ensure that all business units follow standardized procedures for evaluating, documenting and implementing controls. But, keep in mind that processes may vary from business to business. **Develop procedures for identifying and describing why some IT controls vary from unit and unit and have a methodology for standardizing controls where it makes sense.**

Stay Flexible. The rules are still changing and will continue to evolve overtime. **Keep focused on what is best to ensure your IT solution is focused on safeguarding company assets, maintaining data integrity, providing the business with the infrastructure they need to increase shareholder value. SOX 404 compliance is as complicated as creating sustainable network architecture.**

Company Pre-Attestation Process

SOX Audits are not Consistent from One Audit Firm to Another: Unfortunately, the interpretation and implementation of SOX regulation varies greatly. Examples include differing views of appropriate password policies, such as changing passwords every 90 days compared to every 60 days. Some firms may want to see special characters in passwords, while others believe that alphanumeric passwords are sufficient. Established auditor firms realize this and should create a well-defined audit plan. However, because each firm generally considers its methodology proprietary, there will be differences in the audits from one firm to another. **There should not, however, be significant differences, so a good pre-audit should take care of most of your issues and the actual audit firm should incorporate the pre-audit findings into its own, assuming the pre-audit was performed by a legitimate organization.**

A SOX Audit is Not an Audit. The purpose of a SOX audit is to ensure regulatory compliance, not to help you have better security. **The purpose of a SOX pre-audit is to pass the actual one. Most important is that management understands this and ensures the company has everything it needs to pass. Management needs a good pre-audit performed.** Make sure that the company gets good advice that goes beyond a typical SOX audit to help provide recommendations for security beyond your financial systems. **Make sure management has well documented and well performed their pre-audit process so that the results can be used during the actual SOX audit, and lower the cost. Additionally, the penultimate audit is performed by people that you theoretically have more control over; the actual audit is more of an adversarial process.** SOX audits are now a fact of life. You can let them control your security program, or you can become proactive and you can take control. **SOX audits will be performed every year. Accept it as a fact of life, and figure out how to use it for your benefit.**

Auditors Attestation Required by Section 404(b)

Auditor's Attestation: When implementing Section 404, it is important for management to understand the requirements of the auditor. The PCAOB has adopted Auditing Standard No. 2, An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements. This Standard addresses the attestation engagement referred to in SOX 404(b) as well as Section 103(a)(2)(A) of the Sarbanes-Oxley Act, and the

relationship of this engagement to the audit of the financial statements. Auditing Standard No. 2 describes an integrated audit of the financial statements and internal control over financial reporting, resulting in two separate objectives:

1. **To express an opinion on whether the financial statements are fairly stated; and**
2. **To express an opinion on management's assessment of the effectiveness of the company's internal control over financial reporting.**

Auditors Standards: The auditor's attestation of management's assessment of the effectiveness of internal control is referred to as the audit of internal control over financial reporting. The auditor's conclusion about management's assessment will pertain directly to whether the auditor can agree with management that internal control is effective, not just to the adequacy of management's process for determining whether internal control is effective. The auditor must obtain evidence about whether internal control over financial reporting is effective by:

1. **Evaluating management's assessment process;**
2. **Obtaining an understanding of internal control over financial reporting;**
3. **Identifying significant accounts, relevant assertions, and significant processes;**
4. **Evaluating and testing the design of internal controls; and**
5. **Evaluating and testing operating effectiveness.**

Auditors Evaluation: The auditor should evaluate management's assessment process as each phase is completed, or even as each step within a phase is completed, not when the entire process is completed. The auditor will identify controls and their objectives, and will determine whether the controls, if operating properly, would effectively prevent or detect errors or fraud. The auditor's procedures will include inquiry, observation and inspection of relevant documentation. Walkthroughs will be performed for each major class of transactions to confirm the auditor's understanding of the design of controls and their operating effectiveness.

Auditors Assessment of Internal Controls: The auditor must evaluate the implications of the findings from the audit of internal control over financial reporting for the financial statement audit. Where controls are effective, the auditor may be able to alter the nature or timing, or reduce the extent of substantive tests; however, the auditor must still perform substantive procedures for all relevant assertions related to all significant accounts and disclosures during the financial statement audit, and will consider the effect of each control deficiency in designing the nature, timing and extent of those substantive procedures. **The auditor's report must include two opinions as a result of the audit of internal control over financial reporting: one on management's assessment and one on the effectiveness of internal control over financial reporting. Reporting and communication by management and the auditor will be discussed in the final article of the Implementing SOX 404 series.**

Small-Cap SOX Compliance Cost

Based upon various discussions with multiple accounting firms and 404 compliance consultants any small-cap company should anticipate spending at least \$175,000 over 12-18 months and will likely total at least 300 hours of company executive time and at least 700 hours of advisory time. In order to meet SOX 404 compliance, Micro-cap companies should anticipate spending at least US\$75,000 over a 12-18 month period and at least 150 hours of executive company time and at least 350 hours of advisory time, in order to meet SOX 404 compliance. Senior level 404 compliance advisors in the IT and Accounting areas typically bill approximately \$250 per hour, while Technical writers and lower level advisors typically run approximately \$45 per hour. At the very minimum, companies should anticipate hiring at least one full-time employee as the SOX 404 control person, who would report to the company's CFO. This position typically pays between \$50,000-75,000 per year. This is a separate and ongoing cost that is not included in the above noted compliance costs. Additionally, each year consultants will have to re-affirm a company's SOX 404 compliance position and any acquisitions made by companies will have to conform to the SOX 404 standards, requiring added consulting hours. Annual recertification is anticipated to be relatively inexpensive starting as low as \$10,000 per year. Lastly, anticipate that a company's auditors will charge for their initial and ongoing annual certification and attestation that is anticipated to raise a company's existing accounting fees by as much as 100 percent during the initial compliance year and as much as 30% in the following years, excluding any acquisitions.

SOX & Small-Cap Company Compliance, July 17, 2006. © The MacLellan Group, LLC all rights to this publication are reserved. No portion of this report may be reproduced in any form without specific prior written consent of The MacLellan Group, LLC. The information in this document has been compiled from sources The MacLellan Group, LLC. deems to be reliable. The MacLellan Group, LLC. does not hold itself liable for its correctness and any opinions are presented without guarantee. This publication includes confidential and proprietary information and is delivered on the express condition that such information will not be disclosed to anyone except persons who have an actual need to know. No copies or other reproductions of this report may be made without the written consent of The MacLellan Group, LLC. Sources for this White Paper included: Openpages.com, SoxInstitute.com, Network-intelligence.com, Sarbanes-Oxley101.com, EthicsPoint.com, Internet.com, Sarbanes-OxleyForum.com, CIOUpdate.com, GeoTrust.com, Soxcert.org, CorpGovOnline.com, Paisleyconsulting.com, ucdavis.com, nvca.com, accountingobserver.com, SEC.org, Grantthornton.com, law.com, acca.com, whitesoxconsultants.com, Complianceweek.com, kontrak.com, Certus.com, Sun.com, Complianceblog.com, CFO.com, Webcpa.com, SarbOxPro.com, deloitte.com, Faotoday.com, Protiviti.com, Theilia.com, Wikipedia.com, procognis.com, evidian.com, coda.com, cpeonline.com, implexus.com, metagroup.com, essentialsystemsllc.com, Quickbase.com, datamirror.com, knockyoursoxoff.com and Polyproc.com.