



OneNeck White Paper

Sarbanes-Oxley and its Impact on IT Outsourcing

New imperatives for outsourcers in the post Sarbanes-Oxley business environment

By Chuck Vermillion, CEO, OneNeck IT Services

KEY POINTS

All companies — public and private — will have to comply with the spirit of Sarbanes-Oxley.

- A SAS 70 Type II audit is a virtual requirement for IT service organizations as certification of their control processes.
- Not all SAS 70 audits are equal.

EXECUTIVE SUMMARY

Picture yourself at a business symposium where the introductory speaker asks which of the following had the most dramatic impact on United States businesses:

- The digital age
- Outsourcing
- The China price
- The Sarbanes-Oxley Act

While there's no "right" answer to this question, a surprising number of C-level executives would likely choose Sarbanes-Oxley. It's arguably the most significant legislation affecting U.S. business in decades. In just a few years, Sarbanes-Oxley caused dramatic changes in business processes, controls and procedures. It's also completely redefined management's accountability to stakeholders and established criminal penalties for non-compliance. And, while the legislation is directed at public companies, the impact on private companies is undeniable.

That said, this white paper is not about the Sarbanes-Oxley Act, although some basic history and background is presented. Instead, we've taken a look at the ripple effects of the Act on the IT outsourcing community and the new responsibilities and ethics that rest on companies — both public and private — that entrust all or part of their IT environment to an external third party.

Indeed, the rules have changed for IT outsourcing companies and their clients. Sarbanes-Oxley (referred to as SOX herein) casts a giant shadow over every person and organization that comes in contact with a company's financial records and reports, and the controls in place to ensure the accuracy of the information reported.

Beyond demonstrating that their own accounting house is clean, it's clear that public organizations now must ensure that their outsourced business and IT functions and processes comply with the SOX guidelines covering internal controls. Furthermore, private companies should align themselves with the spirit of Sarbanes-Oxley, especially when it comes to outsourcing. In fact, in 2004 the Public Company Accounting Oversight Board (PCAOB) issued a written statement, in which it noted (somewhat ominously), "The use of a service organization does not reduce management's responsibility to maintain effective internal control over financial reporting."

Later in this white paper, we'll look at ways in which outsourcing companies can take proactive measures to meet both the spirit and letter of compliance guidelines through audits such as the well-known SAS 70 and adherence to industry best practices.

"...Simply complying with the rules is not enough. They should, as I have said before, make this approach part of their companies' DNA. For companies that take this approach, most of the major concerns about compliance disappear. Moreover, if companies view the new laws as opportunities—opportunities to improve internal controls, improve the performance of the board, and improve their public reporting—they will ultimately be better run, more transparent, and therefore more attractive to investors."

SEC Chairman William Donaldson

BRIEF HISTORY OF THE SARBANES-OXLEY ACT

On July 30, 2002, the American Competitiveness and Corporate Accountability Act of 2002, commonly known as the Sarbanes-Oxley Act, was signed into law. The Act itself comprises eleven major sections, but includes 1,107 individual sections in all. The act is named after its main architects, Senator Paul Sarbanes and Representative Michael Oxley, and its appearance is usually associated with a series of very high profile scandals, such as Enron and Worldcom, among others.

In announcing the signing of the Act, U.S. President George W. Bush, said, "And now with a tough new law we will act against those who have shaken confidence in our markets, using the full authority of government to expose corruption, punish wrongdoers and defend the rights and interests of American workers and investors."

The President, in referring to the then-new Public Company Accounting Oversight Board, commented, "For the first time, the accounting profession will be regulated by an independent board. This board will set clear standards to uphold the integrity of public audits, and have the authority to investigate abuses and discipline offenders. And auditing firms will no longer be permitted to provide consulting services that create conflicts of interest."

It's generally acknowledged that Section 404 seems to cause the most difficulties for compliance. Beyond simply setting forth new rules and regulations, Sarbanes-Oxley:

- Established new accountability standards for corporate boards, audit committees and independent auditors
- Established a Public Company Accounting Oversight Board (the PCAOB) under the Security and Exchange Commission (SEC)
- Specified civil and criminal penalties for noncompliance.

The creation of the PCAOB alerted everybody in the financial community — and all providers of related services to that community — to the fact that it was, indeed, a new day in terms of who was watching the

numbers. Not only would companies need to be increasingly accurate in reporting their financial results, so too would their auditors need to be diligent in their methodologies. And non-compliance by public companies would now result in something much more severe than a slap on the wrist — it would result in criminal penalties.

The net of compliance cast by Sarbanes-Oxley was massive, and seemed to widen at a regular pace. As the months rolled by, it appeared that everybody in the chain of financial reporting — including outsourcing companies who managed financial systems for clients — would be subject to new levels of scrutiny.

While the benefits are many, the costs of SOX compliance are significant. AMR Research stated in a January 2006 Alert Highlight that since 2003, “... we estimate that companies have spent more than \$14 billion to comply with the law, and that spending will top \$20 billion by the end of 2006.” While the costs of compliance for small-to-medium-sized businesses (SMBs) are high, the operation and business benefits justify the investment.

THE IMPACT OF THE SARBANES-OXLEY ACT ON MID-MARKET AND PRIVATE COMPANIES

Although the Sarbanes-Oxley Act rose to prominence on the wrongdoings of large, public companies, there’s now a new level of expected compliance that cascades down to private companies as well. In short, any private company — large or small — that has a requirement for an audit (especially from a national auditing firm) will likely have to comply with the spirit of Sarbanes-Oxley.

Additionally, many companies that have investments from other than family members will be pressured to conform to Sarbanes-Oxley’s best practices. Why? Because in the long term, it’s unlikely that public accounting firms will have two sets of standards by which they’ll audit, one for public companies and another for private. In the near term, public accounting firms are most likely to recommend Sarbanes-Oxley’s standards as best practices that should be set as goals for private firms, as well as for publicly held companies.

Also impacting SMBs is the fact that accounting firms have been challenged too. Because of a large number of high-profile accounting frauds and bankruptcies, some firms have removed themselves from high-risk audit environments. And while the additional work generated from SOX has resulted in the large accounting firms having more work than they can service, some of these firms have resigned smaller clients due to capacity constraints, or have decided simply to under-serve them.

With all these factors considered, it’s logical to conclude that public accounting firms will view a company that refuses to adopt SOX as high-risk and either drop them from their customer list or refuse to take them on as a new client.

Privately held companies that are planning to go public, grow in revenue, or become acquired also need to seriously consider complying with the

Act as a sign of financial soundness and integrity in reporting. SMBs that do business and partner with public firms governed by SOX are increasingly required by their larger business partners to demonstrate SOX compliance.

We believe that SOX compliance for all companies will become a requirement to stay in business — an “expected behavior” of sorts to maintain the spirit of good business. Compliance ensures solid financial reporting and cannot help but improve business processes. From our perspective, it’s not a matter of “if” your company needs to comply with the Sarbanes-Oxley Act. It’s simply a matter of “when.”

“Here’s what we know about Sarbanes-Oxley: It is one of the most significant changes to federal securities laws in history; it has been difficult and expensive to implement for publicly traded U.S. companies; and it is here to stay. Despite its drawbacks and costs, Sarbanes-Oxley has helped boost shareholder confidence, and it may even boost shareholder value by helping companies operate more efficiently going forward.”

The Gain And Pain Of Sarbanes-Oxley
Colleen Cunningham, Forbes.com

Unfortunately, the SOX compliance pill is harder to swallow for smaller businesses because of the costs associated with the process. With many SMBs working to reduce costs through outsourcing of non-core functions, the pressures of compliance have trickled down to their outsourcing partners. They, too, must now enable compliance within their scope of services, since many IT outsourcers are providing, hosting, or managing the systems through which financial information flows. Without doubt, those systems must now be compliant with the spirit of SOX.

A TOP LINE VIEW OF KEY SECTIONS OF THE SARBANES-OXLEY ACT FOR OUTSOURCING COMPANIES

Of the 70 pages in the Act, the two sections of Sarbanes-Oxley that directly impact IT outsourcing companies are sections 302 and 404. Summaries of these sections follow:

SECTION 302

Corporate Responsibility For Financial Reports

- CEOs and CFOs must personally certify that they are responsible for disclosure controls and procedures and that the report is accurate, complete, and fairly presented.

- Quarterly and annual filings must contain a certification that the CEO and CFO have performed an evaluation of the design and effectiveness of the disclosure controls.
- Certifying executives must state that they have disclosed to their audit committee and independent auditor any significant control deficiencies, material weaknesses or acts of fraud, and significant changes in financial reporting internal controls.

SECTION 404

Management Assessment Of Internal Controls

- Companies must perform an annual evaluation of internal controls over financial reporting and a quarterly evaluation of any material change in the company's internal controls over financial reporting that occurred during the fiscal quarter.
- The company's independent auditor must issue an attestation report on management's assessment of the effectiveness of internal controls over financial reporting.
- Annual filings must contain a report of management on their assessment of the effectiveness of internal controls over financial reporting.

Clearly, the use of an outsourcing company doesn't mean that IT compliance is no longer management's concern. In fact, the PCAOB's Auditing Standard No. 2 specifically addresses the service auditor's reports. It states:

In short — you can't blame the outsourcing company.

Outsourcing doesn't relieve companies of their responsibility to have accurate, compliant systems. If you can't blame outsourcers for passing along errors, then you must ensure they are in compliance as well.

HOW TO DETERMINE IF YOUR OUTSOURCED SERVICES ARE SUBJECT TO SOX COMPLIANCE

To help determine if the work you're outsourcing to a service organization is subject to SOX compliance, The American Institute of Certified Public Accountants Professional Standards AU 324, Service Organizations, advises as follows:

A service organization's services are part of a company's information system if they affect any of the following:

- The classes of transactions in the company's operations that is significant to the company's financial statements
- The procedures, both automated and manual, by which the company's transactions are initiated, authorized, recorded, processed, and reported from their incurrence to their inclusion in the financial statements
- The related accounting records, whether electronic or manual, supporting information and specific accounts in the company's financial statements involved in initiating, authorizing, and recording, processing, and reporting the company's transactions
- How the company's information system captures other events and conditions that are significant to the financial statements
- The financial reporting process used to prepare the company's financial statements, including significant accounting estimates and disclosures

Beyond being responsible for compliance, the lack of definition on what outsourcing organizations must do to show compliance leaves room for misinterpretation. After all, the Sarbanes-Oxley Act is a concept, not a rules-based regulation. However, careful companies will find a host of standards already in place with some — such as CobiT® (Control Objectives for Information and related Technology) — dating back to 1996.

Without strict guidelines, organizations are taking different strategies to the application of compliance requirements for outsourced processes and engagements. For example, two separate META Group studies conducted in 2004 found that nearly 25 percent of organizations were ignoring outsourced functions and processes in first year SOX efforts — a red flag for potential audit exceptions.

In June of 2004, the SEC added a bit of clarity to the issue of outsourcer compliance when it approved the PCAOB Auditing Standard No. II, "An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements." The standard addresses both the work required to audit internal control over financial reporting, as well as the relationship of that audit to the audit of the financial statements.

"The use of a service organization does not reduce management's responsibility to maintain effective internal control over financial reporting. Rather, management should evaluate controls at the service organization, as well as related controls at the company, when making its assessment about internal control over financial reporting."

THE RELATIONSHIP BETWEEN SAS 70 AUDITS AND SOX COMPLIANCE

SAS 70 is an auditing standard developed by the American Institute of Certified Public Accountants for service organizations. As it relates to outsourcing IT, a SAS 70 audit is the means through which an auditor examines an outsourcer's control activities, particularly around IT and related processes.

A SAS 70 type II audit is widely recognized because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes. The requirements of Section 404 of the Sarbanes-Oxley Act make SAS 70 audit reports even more important to the process of reporting on effective internal controls at outsourcing organizations.

The PCAOB states that Statement of Auditing Standards No. 70 (SAS 70), Service Organizations (AU section 324) applies to the audit of financial statements of a company that obtains services from another organization that are part of its information system. In short, PCAOB

Industry Guidelines for Sarbanes-Oxley Compliance			
Industry Guideline	Advantages	Disadvantages	OneNeck®
CobIT (Control Objectives for Information and related Technology)	<ul style="list-style-type: none"> • Wide range of control objectives (34) • Platform independent 	<ul style="list-style-type: none"> • Too broad • Too expensive to audit 	
ITGI (IT Governance Institute 2004 Report)	<ul style="list-style-type: none"> • 12 Key controls directly related to financial reporting 	<ul style="list-style-type: none"> • Excludes operational and efficiency controls 	
AICPA (American Institute of Certified Public Accountants)	<ul style="list-style-type: none"> • Refined number of control objectives to 7 • Applicable to any IT service organization • Developed the "Statement on Accounting Standards No. 70," or "SAS 70 Audit" • Two SAS Audits exist: Type I and Type II 	<ul style="list-style-type: none"> • SAS 70 Type I Audit is not tested by auditors and cannot be used for SOX compliance • SAS 70 Type II Audit is expensive for outsourcing firms 	<div style="border: 1px solid black; padding: 2px; display: inline-block;">X</div> (SAS Type II Audit)

Auditing Standard No. 2 indicates that evidence about the operating effectiveness of controls at a service organization can be obtained from a Type II SAS No. 70 report.

In other words, the auditing firm for an enterprise who has outsourced its IT function can rely on a SAS 70 Type II audit report as evidence that specific control objectives are appropriately designed and functioning. If the scope of the control objective matches the company's requirements, the audit report can be relied on.

With this brief background, it's easy to understand why the SAS 70 Type II has attracted so much attention from outsourcing companies. A SAS 70 Type II examination signifies that a service organization has had its control objectives and control activities examined by an independent auditing firm. A formal report including the auditor's opinion is issued to the service organization at the conclusion of a SAS 70 Type II examination, which can then be supplied by the services organization to its outsourcing clients.

"Of those with more than one service provider, approximately 43 percent of companies plan to use a Service Auditor Report, an opinion based on Statement on Accounting Standards No. 70 (SAS 70)."

Emerging Trends in Internal Controls
Ernst & Young

NOT ALL SAS 70 AUDITS ARE CREATED EQUAL

As it develops its compliance plan, a company, along with its auditors, should look at the details of the SAS 70 Type II report to do an apples-to-apples comparison. It's important to understand the scope of an audit in order to accurately compare and evaluate outsourcers. Plus, the scope of work provided by the outsourcing company and the control objectives for the SAS 70 Type II must match. If they don't, the SAS 70 Type II cannot be counted on by management to demonstrate full compliance with SOX and further audits would be required.

For example, a comprehensive application outsourcing agreement includes seven service components. It's possible to have a SAS 70 Type II audit done on only three of the areas: the physical data center, the network, and the operating system. But if the service provider is also managing middleware, databases, and applications, those areas must be included in the scope of the SAS 70 Type II audit for it to satisfy those requirements.

In short, not all SAS 70 Type II audits are alike. The service providers themselves define which control objectives are to be examined in the report, and the options are many. The widest range of control objectives are found in CobIT 4.0, a set of guidelines and best practices that were developed in the mid-1990s. CobIT was widely accepted because it's platform independent.

However, in a post-SOX environment with increased scrutiny on IT controls, CobIT's 34 control objectives were considered by many to be too broad and too expensive to audit. In the IT Governance Institute's (ITGI) 2004 report, "IT Control Objectives for Sarbanes-Oxley," 12 key control objectives were identified, and the report's preface noted:

"Many IT controls were considered in developing this document. However, a significant effort was made to limit the discussion of such controls to those more directly related to internal control over financial reporting. As such, this document is deliberate in its exclusion of controls supporting operational and efficiency issues. It is, however, inevitable (and desirable) that operational and efficiency issues will be addressed over time and built into the control structures and processes that are developed."

In refining the number of control objectives that should be included in a thorough SAS 70 Type II audit, the AICPA's (American Institute of Certified Public Accountants) Audit Guide, "Service Organizations: Applying SAS No. 70," lists seven controls. The Guide suggests that the seven IT Control objectives may be applicable to any service organization that uses IT in providing services that are part of a user organization's information system.

In summary, we've gone from CobIT's 34 to ITGI's 12 to AICPA's seven suggested control objectives to be audited as part of a SAS 70 Type II report at IT outsourcing providers. However, the list of audit options

SAS 70 Type II Control Objectives	Service Provider Type				
	Colocation Provider	Managed Hosting Provider	Application Service Provider	Remote Services Provider	OneNeck
Organization and Management Control Equipment	X	X	X	X	X
Computer Operations	X	X			X
Incident Management		X	X		X
Systems Change Management			X		X
Applications Development and Control					X
System, Database, Application and Network Security			X	X	X
Environmental Control and Monitoring Devices	X	X			X
Physical Access to Buildings	X	X			X

doesn't end with selecting a number of control objectives. That's because within the realm of SAS 70 reports, there are Type I and Type II audits.

A SAS 70 Type I is a point-in-time, snapshot audit that focuses on general and application controls but does not include testing by auditors. A Type II audit occurs over a period of time (typically six months to a year), focusing on general and operational controls during a life cycle, with auditors typically performing actual testing. A Type II is generally more expensive as well as more burdensome for the outsourcer. Since a Type I is only a snapshot in time it cannot be used to satisfy SOX control requirements. In short, only a Type II audit can be relied upon by an auditor.

SAS 70 engagements are generally performed by control-oriented professionals — Service Auditors — who have experience in accounting, auditing, and information security. A SAS 70 engagement allows a service organization to have its control policies and procedures evaluated and tested (in the case of a Type II engagement) by an independent party. Very often this process results in the identification of opportunities for improvements in many operational areas.

User organizations — companies who outsource all or part of their IT environment — should provide a Service Auditor's Report of their outsourced business processes to their auditors. This will greatly assist the company's auditor in planning the audit of the user organization's financial statements. Without a Service Auditor's Report, the company would likely have to incur additional costs in sending their auditors to the service organization to perform their procedures.

At OneNeck, we believe the importance of doing business with a SAS 70 Type II-audited outsourcing partner has never been greater. Here's why:

- The Sarbanes-Oxley Act and other sets of guidelines have clearly communicated that if your accounting function is outsourced, you must still treat it as if it were your own.
- Management must have an understanding of the outsourcer's controls and test procedures, and certify that they are materially accurate.

- Executives have to stand behind the validity of the outsourcer's tests.

Clearly, if you're going to outsource your IT function, it's imperative to outsource to a SAS 70 Type II partner, or implement your own testing and certification program on a quarterly basis for public companies. With neither a SAS 70 Type II audit nor thorough testing by a third party, you could be positioning yourself for criminal investigation.

ONENECK'S APPROACH TO COMPLIANCE

At the time of the introduction of Sarbanes-Oxley, we believed it was imperative to provide as much assurance to our customers as possible that our practices and methodologies were compliant with the spirit of the Act. We adopted a two-pronged approach comprising ITIL® best practices and a SAS 70 Type II audit.

ITIL — the IT Infrastructure Library — is a series of documents that are used to aid the implementation of a framework for IT Service Management.

ITIL currently comprises several sets that are divided into two main areas: Service Support and Service Delivery. Service Support is the practice of those disciplines that enable IT Services to be provided effectively. Service Delivery covers the management of the IT services themselves. We rigorously follow the best practices set forth by ITIL.

We believe that ITIL will become the de facto standard of best practices for IT service providers. From our vantage point, ITIL is to IT, as GAAP is to accounting. In many ways, ITIL is more difficult to comply with than a SAS 70 Type II audit.

That said, in addition to adhering to the guidelines and concepts of ITIL, we've made a substantial investment in a SAS 70 Type II audit for the benefit of our customers and their auditors. We believe that in a world without specifications to which outsourcers must comply, everything we can do to put our customers at ease is well worth the investment. To us — and more importantly, to our customers — the SAS 70 Type II is a security blanket over ITIL's best practices and serves to reduce the overall compliance costs of our customers.

As described in the previous section, the number of control objectives included in the SAS 70 is usually at the discretion of the service provider. We chose to add an additional control objective covering management to the AICPA's list of seven recommended control objectives.

Control objectives for OneNeck's SAS 70 Type II are:

1. Management Control Environment
2. Computer Operations, including SLA Management
3. Incident Management
4. Systems Change Management
5. Applications Development and Control
6. System, Database, Application and Network Security
7. Environmental Control and Monitoring Devices
8. Physical Access to Buildings

IT professionals, especially those in executive positions, need to be well versed in internal control theory and practice to meet the requirements of the Sarbanes-Oxley Act. CIOs must now take on the challenges of (1) enhancing their knowledge of internal control, (2) understanding their organization's overall Sarbanes-Oxley compliance plan, (3) developing a compliance plan to specifically address IT controls, and (4) integrating this plan into the overall Sarbanes-Oxley compliance plan.

IT Control Objectives For Sarbanes-Oxley
The IT Governance Institute

With this double layer of certification and accepted standards in place, we have, in effect, pre-certified OneNeck's services. This kind of certification saves our customers money by eliminating a step of the audit process for which they would typically have to pay. By completing the SAS 70 Type II audit — and exceeding AICPA standards — we have a much better sense of the compliance process and can therefore better advise our clients.

As does every company that completes Sarbanes-Oxley compliance or a SAS 70 audit, we gained certain operational benefits from the process. However, SOX compliance is not a topic on which organizations can rest. Indeed, the nature of corporate accounting and financial controls has forever been changed by Sarbanes-Oxley legislation that just might be the most influential business event of the past 100 years.

GLOSSARY OF TERMS

AICPA (American Institute of Certified Public Accountants): An accounting industry group that developed the SAS 70 "Statement on Accounting Standards No. 70." The statement outlines two audit types — the SAS 70 Type I and the SAS 70 Type II. In its Audit Guide, "Service Organizations: Applying SAS No. 70," the group refined the number of control objectives that should be included in a thorough SAS 70 Type II audit to seven.

CobiT® (Control Objectives for Information and related Technology): A set of IT guidelines and best practices developed in 1996.

ITGI (IT Governance Institute): This industry group published 12 key control objectives in its 2004 report, "IT Control Objectives for Sarbanes-Oxley." The report limited controls to those directly related to internal control over financial reporting. The ITGI document deliberately excluded controls supporting operational and efficiency issues.

ITIL (IT Infrastructure Library): A series of documents used to implement a framework for IT Service Management. The library includes service support and delivery. ITIL for IT can be compared to GAAP for accounting.

PCAOB (Public Company Accounting Oversight Board): An independent board created with the Sarbanes-Oxley Act to regulate the accounting industry. This board sets clear standards to uphold the integrity of public audits. In addition, it has the authority to investigate abuses and discipline offenders.

Sarbanes-Oxley Act (SOX): Also known as the American Competitiveness and Corporate Accountability Act of 2002, Sarbanes-Oxley was signed into law on July 30, 2002. The Act established new accountability standards for corporate boards, audit committees and independent auditors. In addition, it created the Public Company Accounting Oversight Board, as well as specified civil and criminal penalties for noncompliance.

SAS 70 (Statement on Accounting Standards No. 70): An auditing standard developed by the American Institute of Certified Public Accountants for service organizations. As it relates to outsourcing IT, a SAS 70 audit is the means through which an auditor examines an outsourcer's control activities, particularly around IT and related processes.

SAS 70 Type I Audit: A point-in-time, snapshot audit that focuses on general and application controls but does not include testing by auditors. It cannot be used to satisfy SOX control requirements.

SAS 70 Type II Audit: An independent auditing firm examines a service organization's control objectives and control activities. The auditor issues a formal report including the auditor's opinion to the service organization at the conclusion of the examination, which can then be supplied by to clients. The service providers define which control objectives to examine. A Type II audit occurs over a period of time typically lasting six months to one year.



5301 North Pima Road, Suite 100
Scottsdale, Arizona 85250
Fax (480) 609-4308
info@OneNeck.com