

Working through Sarbanes-Oxley compliance and outsourcing IT services

White paper

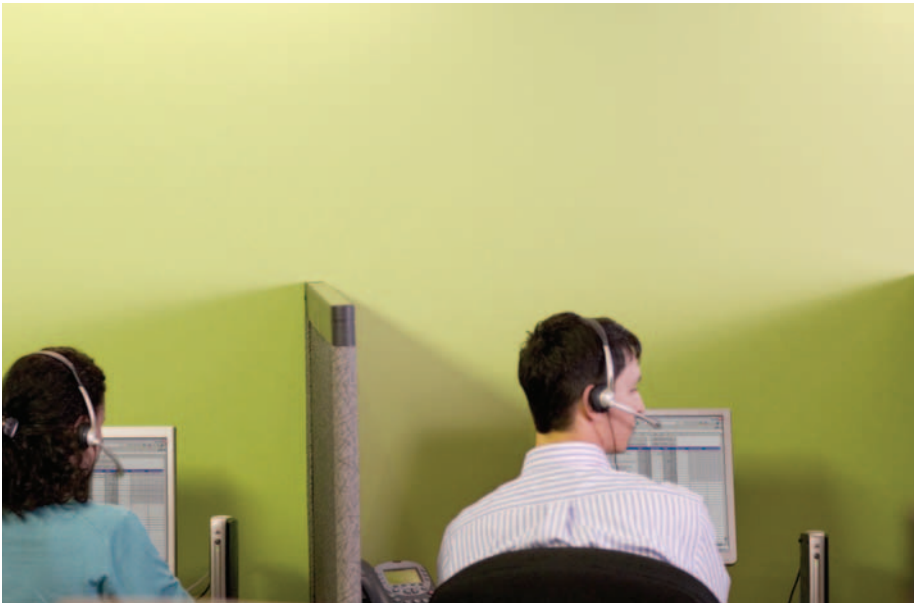


Table of contents

- The challenge**2
 - A company can't outsource its responsibility2
- Addressing the challenge**2
 - Understanding the impact on financials2
 - Step 1-Identify what to monitor2
 - Step 2-Determine how to monitor3
 - Step 3-Check and refine controls3
 - Step 4-Ensure continuous improvement3
- SAS 70 audits**4
- Conclusion**4
- To Learn more**4

The challenge

A company can't outsource its responsibility

As more companies become familiar with the dictates of the Sarbanes-Oxley Act (SOX), they are becoming more comfortable outsourcing certain IT functions. Outsourcing can help a company comply in a way that reduces cost, removes complexity and lowers the burden on internal staff members. Many companies now view an outsourcing provider as an extension of their in-house resources for managing their SOX compliance responsibilities.

While outsourcing arrangements offer compelling business benefits, they also pose special challenges for a management team. A company that plans to enter an outsourcing relationship needs to assess its complete control structure—including all in-house and outsourced portions. The assessment process should determine whether the controls are sufficient, adequately documented and consistently performed, and how they will impact business processes.

It's important that managers gain a close understanding of their controls. That's because the responsibility for confirming the adequacy of outsourced controls remains with the company and its executive management team, not with the outsourcing provider. The Sarbanes-Oxley Act and the Public Company Accounting Oversight Board preclude the delegation of management's responsibility for compliance.

So how does an organization assess and confirm outsourced controls? In short, it must put a process in place to assess risks and to develop appropriate controls and audit measures for outsourced services. Through this process, a management team establishes a system of checks and balances that allows it to verify that outsourced services are meeting the company's requirements.

Addressing the challenge

Understanding the impact on financials

Whether a company is already outsourcing work or is still evaluating outsourcing, it must determine which outsourced services need to be examined and audited. To do so, managers should ask a simple question: "Do the functions being outsourced affect financial reporting and, in particular, the underlying control structure?" If the answer is yes, a company needs to have oversight in place to confirm that its controls are effective.

Once the management team has identified the areas requiring focus, it can move forward in a step-by-step manner.

Step 1— Identify what to monitor

At the outset, a company needs to determine the areas that have financial reporting significance, including business processes, and the associated applications and supporting infrastructure.

The company is then positioned to identify the applicable control objectives and requisite key controls that provide assurance that its financial reporting is complete, accurate, authorized, timely and secure. This includes determining those controls that the company has entrusted or is considering entrusting to its outsourcing service provider. At this point, it is critical that gaps or differing assumptions between the organizations are identified and rectified.

When a company is in an outsourcing relationship, many IT internal controls that would have normally been performed in house are transferred to an outside service provider. This means the company's internal controls assessment will need to reference some of the outsourcing provider's internal controls.

Initially, the management team will want to confirm before or within the outsourcing agreement that its service provider has controls in place that satisfy the company's requirements. As the client, the company needs to know that its provider's controls are functional and robust.

The HP approach: As a first step in outsourcing Sarbanes-Oxley compliance needs, an HP team meets with the client's SOX team to conduct a complete review of the organization's situation. This allows both teams to jointly identify the outsourcing services that best meet the client's needs. HP also helps determine what controls are needed.

Step 2—Determine how to monitor

Once a company knows what it needs to monitor, it must determine the how. Specifically, this step addresses the question of how the company will assess and monitor its outsourcing provider's controls to make sure they continue to be effective.

This includes identifying key indicators and periodic checks and balances that will alert managers to possible malfunction of controls. This information is typically spelled out in a broader governance plan that guides the overall relationship with the outsourcing provider.

In general, a company should determine its audit needs and then work with its supplier to determine how best to meet those needs. These should be included within the audit rights clauses of the outsourcing agreement. There are many ways to gain the assurance that the outsourcing provider has effective internal controls in place. These can include one or more of the following steps, along with approaches not listed here:

- Certify the process in-house using the company's internal or external auditors. It may make sense to audit a service provider if the company has substantial control over the outsourced processes. In these cases, the audit may be looked at as an extension of normal audit procedures. It is important to put such audit provisions in contractual agreements with this type of service provider. Even if the controls are standard, it may still make sense for the company to carry out an audit.
- Have the outsourcing provider participate in a SOX compliance project run by the company to document and internally test the relevant internal controls over the applicable systems.

- Request and obtain a third-party assurance document, such as a SAS 70 or Section 5900 audit conducted by the company or its supplier's auditor. If this is the case, a company typically augments its provider's SAS 70 audit with work carried out by the company's internal audit staff or an outside audit firm.

The HP approach: Once an organization's needs and controls are identified, HP works with the company's SOX team to help identify specific risks and controls associated with the processes in question.

Step 3—Check and refine controls

At this point, it's time to fine-tune controls. The company works with its outsourcing provider to change controls if they are insufficient in terms of allowing the company to maintain effective control over its financial records and reporting. In addition, the company will want to discuss the allocation of any costs associated with the changes made in this step.

Through this process, a company needs to gain the assurance that its outsourcing vendor has effective systems and processes in place. That's because deficiencies in the outsourcing provider's controls could prevent the management team from making an affirmative statement as to the effectiveness of its controls over financial reporting.

The HP approach: HP closely monitors all controls that have been outsourced to HP to verify that they meet the agreed-upon requirements. Additionally, all controls are subjected to periodic testing as determined by the client's internal SOX team in consultation with HP professionals.

Step 4—Ensure continuous improvement

An outsourcing provider should work closely with its client to improve controls on an ongoing basis. Simply verifying the process after implementation is not enough. Monitoring of control effectiveness must continue during the relationship, because outsourced functions and the processes used to perform them inevitably evolve to meet changing needs.

Given this reality, a company and its provider should continually monitor controls and make adjustments as the need arises. The outsourcing implementation should allow an organization to adapt to changes as they occur.

Although outsourcing providers have no direct compliance obligations under Sarbanes-Oxley, the provider should understand the risks associated with non-compliance and should work actively to help its client assess and mitigate those risks.

The HP approach: As changes or deficiencies are noted, HP works with the client's SOX team to amend the system and processes in a timely manner to maintain continuous compliance.

Through all of these steps, HP strives to deliver quantifiable and predictable business outcomes by using structured service level agreements (SLAs). These SLAs are linked to key performance indicator metrics to allow an objective evaluation of HP's performance.

These measures work alongside disciplined reporting and formal governance processes to assist and support an organization's Sarbanes-Oxley compliance program.

SAS 70 audits

In many SOX outsourcing relationships, a SAS 70 audit is useful. SAS 70, which was developed by the American Institute of Certified Public Accountants (AICPA), is recognized by Section 404 of the Sarbanes-Oxley Act.

A SAS 70 audit typically addresses critical metrics, such as the completeness, accuracy and timeliness of internal controls and activities. While a company and its auditors may not rely solely on SAS 70 reports for purposes of their Section 404 assessments, the reports may be used as supporting evidence.

There are two types of SAS 70 audit reports. Type I covers internal controls for a specific point in time. Type II covers a specified period and typically runs for six to twelve months, although other periods can be used. A Type II SAS 70 with a minimum period of six months is required to be used as part of a customer's attestation of an outsourcer's controls. At its heart, a SAS 70 review is not a final step, but rather a piece of an ongoing auditing process.

The HP approach: HP retains a global audit firm to perform Type II SAS 70 reviews for many of HP's delivery centers. After publication, HP reviews the results with its clients.

Conclusion

Increasingly, companies are turning to outsourcing in the hopes of reducing the cost and complexity of their operations. The Sarbanes-Oxley Act has not diminished interest in outsourcing. Companies can view outsourcing providers as supportive in their compliance efforts. The potential benefits are enabled when a company logically facilitates its compliance effort in concert with an outsourcing provider.

These and other gains don't come without management challenges, however. To achieve a successful outsourcing relationship and position an organization for SOX compliance, a company needs to gain a clear understanding of what it is going to monitor, how it will do the monitoring, and how it will refine and strengthen its controls on an ongoing basis.

The step-by-step process outlined in this paper can help put an organization on the path to a successful outsourcing relationship. HP professionals follow this same general process when they assist clients with their outsourcing and compliance needs.

While at a root level, the responsibility for compliance remains with the company and its managers, HP professionals understand how to support an organization's efforts to meet its legal and regulatory responsibilities under the Sarbanes-Oxley Act.

To learn more

To learn more about HP's outsourcing services, please visit www.hp.com/go/outsourcing. For further information on how HP can help with the Sarbanes-Oxley Act and other regulations affecting outsourcing, please contact your HP representative or outsourcing@hp.com.

For more information visit: www.hp.com/go/outsourcing.

© Copyright 2006 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA0-3762ENA, January 2006

