Gartner Research

Publication Date: 24 April 2008 ID Number: G00157234

Sarbanes-Oxley Update: How to Best Support the CFO

French Caldwell, John E. Van Decker

CFOs worldwide are affected by the U.S. Sarbanes-Oxley Act (SOX) and similar directives in other countries. Having dealt with SOX longest, CFOs of large and midsize firms registered with the U.S. Securities and Exchange Commission (SEC) are giving it less attention. When they do, it is on "financial governance," which, with the right IT support, promises improved business performance.

Key Findings

- The new Public Company Accounting Oversight Board (PCAOB) Audit Standard No. 5 (AS5) and related SEC guidance changed the SOX internal-control audit to a goal-based, top-down risk-oriented method. This enables a lower compliance cost entry point for firms with less than $75 million of capitalization when they're due to file SOX Section 404 in 2009 or 2010, and large and midsize firms to scale down their programs.
- Few CFOs will avoid SOX and similar directives. SOX-like regulations will appear globally in a SOX "knock-on effect."

Recommendations

- Before moving to financial governance investments, focus IT solutions for the CFO on improving compliance program management. Move compliance processes off spreadsheets and file servers onto an enterprise governance, risk and compliance (EGRC) platform with a common repository for SOX compliance documentation, good workflow and flexible reporting. The next priority is IT solutions for segregation of duties and transaction monitoring for ERP.
- When moving to financial governance, shift IT support to critical financial processes, such as financial close and reconciliation. These investments target key aspects of SOX compliance and can provide direct performance improvements.
- Ensure that CFOs and supporting IT managers who are prepping for compliance (nonaccelerated filers to the SEC, Japanese and European registrants responding to similar directives and firms dealing with industry-specific variations, such as the Model Audit Rule for U.S. mutual insurance firms) learn from counterparts who have made IT investments for SOX.

TABLE OF CONTENTS

LIST OF FIGURES

ANALYSIS

For CFOs and their IT support managers who are just getting started with SOX and similar directives worldwide, there is much to learn from the transition taking place in technology support for SOX. For CFOs who have been conducting SOX compliance for two or three years, SOX may no longer be a top-of-mind issue, but, to cut audit costs and improve business performance, it is important that they take time to consider IT investments that make the most of recent regulatory and audit standard changes.

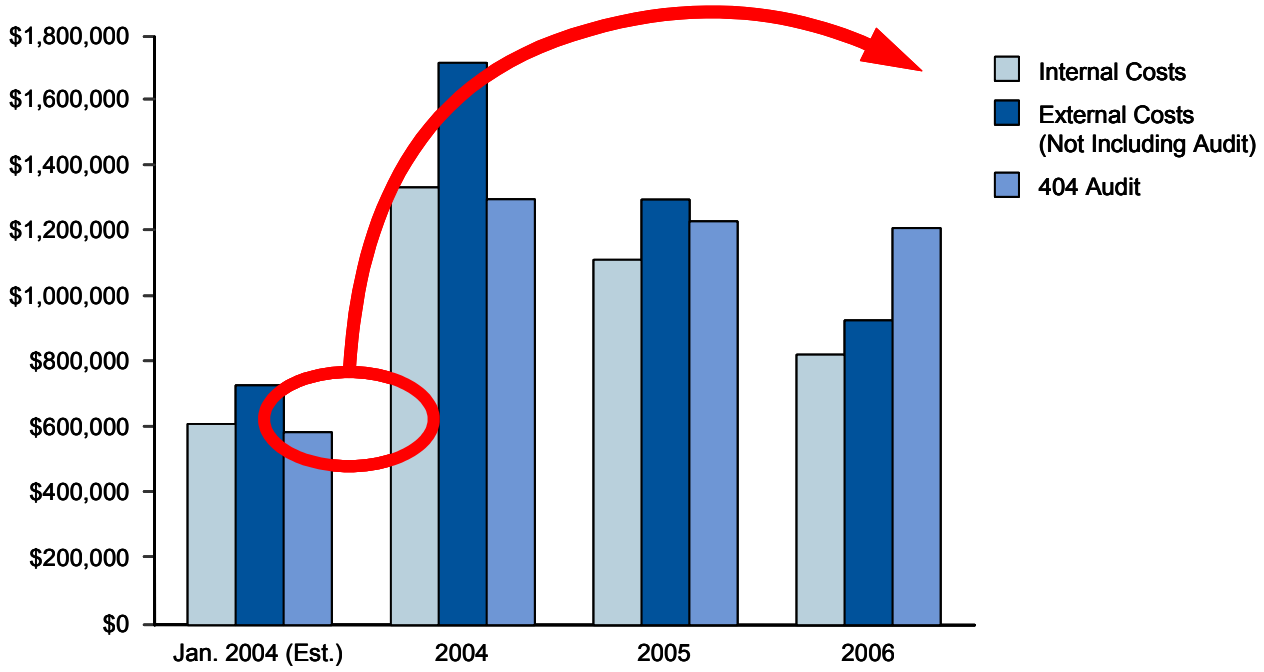
The trailing costs for the processes SOX has created are a legacy with which most firms do not want to be burdened. Some enterprises have created lots of manual processes to meet SOX requirements and avoid material deficiencies. However, many have moved on to more-pressing issues, such as generating revenue by trying to become more of a value-added business partner and improving corporate performance management (CPM) initiatives. For wise firms, SOX has changed the way the office of the CFO does business — these firms are working more closely with the IT, legal and internal audit departments, and their processes are more transparent, consistent and measurable. With the application of new financial governance technologies, executives have more-accurate and timelier information on risks, as well as improved control over processes in what Gartner describes as the "last mile of finance" (see "Taking a Holistic Approach to the Last Mile of the Financial Close").

However, CFOs know that SOX is not yesterday's issue — it is still important, but changes in audit standards and regulatory guidance have reduced the level of effort of compliance. A real advantage for firms will occur less around ensuring compliance and more on improving governance and optimizing business processes to reduce waste, revenue leakage and operating inefficiencies.

1.0 The Impact of PCAOB AS5

From 2004 through 2006, overall spending on SOX dropped, implying that many companies invested in the systems and processes to implement and manage SOX compliance. However, the Section 404 internal-control audit component hardly budged (see Figure 1), implying that this investment has not affected the level of effort external auditors expend in evaluating internal controls.

Figure 1. Internal and External SOX Costs Are Down, But Audit Hasn't Budged



2004 Through 2006 SOX Spending, Mean
(Based on $5 billion to $7 billion annual revenue)

Source: Financial Executives International

Because they were accountable directly to the SEC for reporting on the status of management's control processes, most auditors felt compelled to take a highly granular approach to the Section 404 audit. The costs of auditing, particularly as small businesses approached their own SOX deadline, became a political issue and a potential threat to the competitiveness of U.S. equities markets. Much attention also was focused on a post-SOX decrease in initial public offerings (IPOs) on U.S. exchanges and on the increase of IPOs on London exchanges. Although much of the media attention on IPOs was hype, and not all the shift to London was attributable directly to SOX costs, the SEC's first significant relaxation of SOX rules in December 2006 shifted SOX deadlines for newly listed companies to allow them to skip SOX reporting in their first post-listing annual reports.

Continued pressure to lower audit costs led the PCAOB to release AS5 in May 2007. The effect of the new audit standard was the establishment of an equitable balance of power between audited entities and their external auditors, enabling a significant rescaling and downsizing of the Section 404 audit. The new audit standard significantly influences IT support for the office of the CFO in four ways:

1. The focus shifted to entity-level controls, including those over the period-end financial reporting process, which Gartner describes as the "last mile of finance."
2. AS5 and related SEC guidance to companies encourage a risk-oriented approach to internal controls.
3. Attention to management efforts on anti-fraud controls is emphasized.

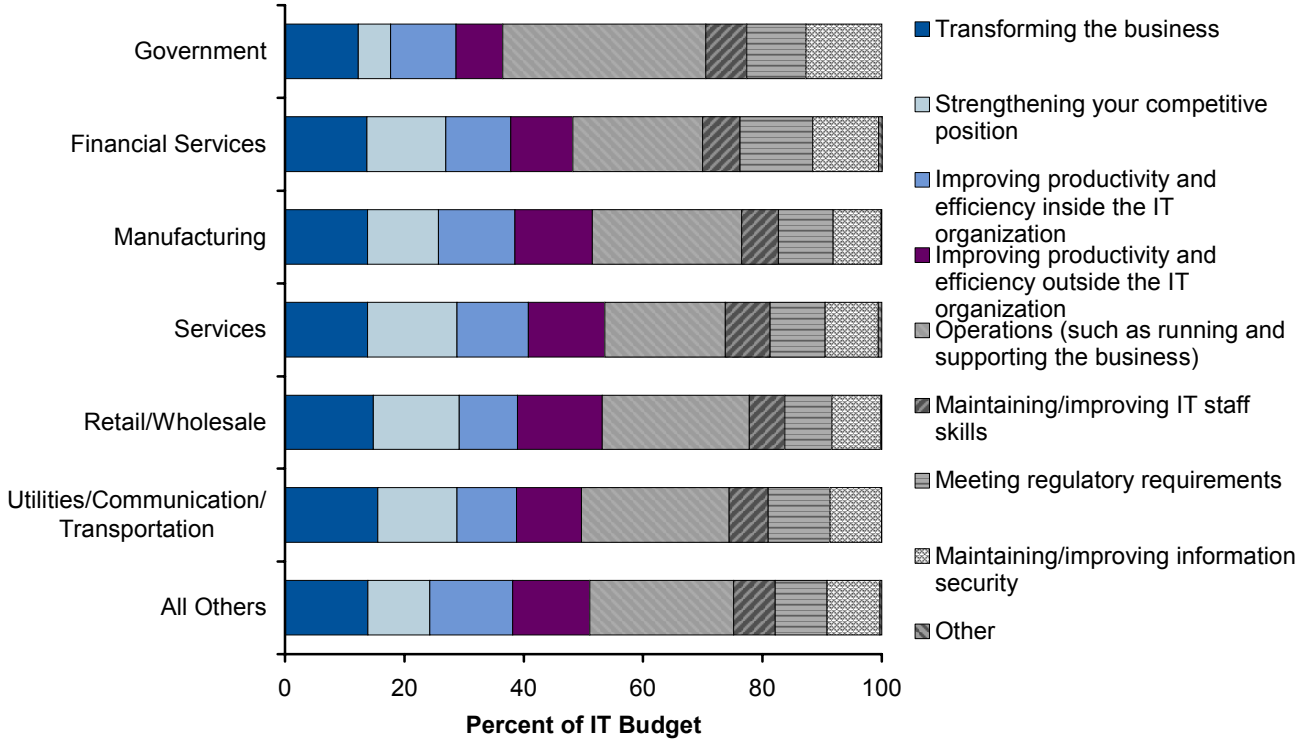
4. Automated controls can be benchmarked and audited only when there are changes.

The overall effect of AS5 on the office of the CFO has been to shift management attention on compliance to financial governance — which, besides the potential to lower audit costs, also has direct performance benefits. IT support for the CFO also should address investments in financial governance solutions, including the automation of period-end processes, risk management and the automation of transactional controls, especially anti-fraud controls.

2.0 The Lasting Technology Impact of SOX

The obvious downsides of SOX are the added expense for compliance programs, the growth of internal-audit and external-audit services, and new governance, risk and compliance (GRC) IT spending. The estimate from Financial Executives International was that, in 2006, SOX costs averaged $2.9 million (see "FEI Survey: Management Drives Sarbanes-Oxley Compliance Costs Down by 23%, But Auditor Fees Virtually Unchanged"). A Gartner survey in late 2006 showed that regulatory compliance costs, not just SOX, were 9.5% of the IT budget (see Figure 2), but the trend was downward from a 2005 survey showing that SOX compliance alone took more than 10% of the IT budget.

Figure 2. Percent of IT Budget



Source: Gartner (April 2008)

Despite downward cost trends, compliance costs and the diversion of management attention are the downsides of SOX for the CFO and for IT professionals who support the office of the CFO. So, what is the upside? In the long term, SOX has had an overall positive impact on the availability of reliable financial information and on the consistency and integrity of critical processes in the last mile of finance. For the savvy firm, the office of the CFO is benefiting with better, timelier information for business decision making. Most of the benefits have been derived from applying IT solutions in response to audit deficiencies, which has focused the CFO not only on compliance but also on risk management and on improving financial governance. SOX expenditures have resulted in significant improvements in the reliability and transparency of much of the financial IT infrastructure, although these improvements rarely reach that financial last mile, which is the consolidation and reconciliation processes — the point at which financial processes are most likely to be violated.

The office of the CFO's first technology investments typically are done in conjunction with internal audits. The focus is on adding transparency to compliance management and on reducing the amount of manual labor dedicated to compliance activities, which leads to buying solutions for GRC management and to automating the monitoring of common ERP controls such as segregation of duties. GRC management solutions such as those offered by EGRC platform vendors OpenPages, Paisley, Oracle, BWise, MetricStream enable improved workflow and documentation of compliance and audit processes, as well as risk management processes that enable a lower-cost, risk-oriented approach to compliance.

Controls automation and monitoring, including segregation of duties solutions, offered by ERP vendors SAP, Oracle, Approva, Security Weaver and others enable a reduction in the manual sampling of financial transaction data and improvement in the reliability of transactional controls. The office of the CFO and internal audit also have found common ground on investments in audit analytics solutions from vendors such as ACL Services and Oversight Systems, enabling ad hoc analysis of transactional data and continuous control monitoring. At times, the CFO chose not to wait for IT support to implement GRC solutions, resulting in significant gains for software-as-a-service vendors such as Axentis, Compliance 360 and BI.

Investments in EGRC and segregation of duties are short-term choices that do not address the issues that will remain in the last mile of finance. GRC management solutions can help in some areas, and CPM applications (such as financial consolidation) can improve some processes. However, most organizations have addressed the immediate concerns of SOX and are looking to improve controls over the last mile of finance by implementing a broader approach to managing governance and compliance in the finance function. This path has led to the emergence of a new market of solutions that Gartner has defined as financial governance, combining elements of ERP, EGRC and CPM suites.

SOX audits of internal controls have revealed that many financial organizations have poorly controlled processes in the last mile of finance — that is, the consolidation and reconciliation processes, which are crucial to the accuracy and timeliness of financial reporting — the basic intent of SOX. In enterprises with multiple entities, these processes vary and often were carried out via user-defined applications built on Excel spreadsheets. Gathering the data into a common reporting format for the enterprise often took longer than the consolidation and reconciliation processes at the individual entities.

To improve and standardize processes across entities, enterprises invested in financial consolidation as part of CPM solutions from vendors such as Oracle and SAP, and financial close and reconciliation solutions from vendors such as Trintech. In cases where moving from spreadsheets is not feasible or desired, the office of the CFO can acquire spreadsheet control products from vendors such as Cimcon Software, Compassoft and Prodiance to ensure that all

entities are employing the same user-defined application, controlling all modifications and ensuring auditability.

Financial governance solutions form a new market that will emerge during the next three to five years, combining elements of ERP, finance GRC management and CPM suites. These solutions will build additional process controls around financial consolidation to support financial close processes and the production of periodic financial statements for regulators. It will augment the compliance controls in finance GRC solutions with broader controls that monitor capabilities, and when delivered as a comprehensive solution, will enable CFOs to better manage financial risk. However, as financial governance solutions mature, CFOs will face the challenge of addressing their most-pressing governance issues with varied point solutions (see Figure 3).

Figure 3. Financial Governance Examples

Financial Governance Components	CPM Vendors	Financial Governance Specialists
Financial Consolidations and Reporting	All CPM vendors	None
Interentity Transaction Management	ERP vendors (SAP, Oracle and Lawson)	None
Reconciliation Management	Most offer intercompany reconciliations only	Trintech
Financial Controls and Compliance	ERP vendors (SAP, Oracle and Lawson) Some CPM vendors considering offerings	Axentis, OpenPages, Paisley, BWise, MetricStream and other EGRC platform vendors
Financial Close Management	Oracle and SAP Some CPM vendors have limited offerings	Trintech
Access Controls, Segregation of Duties	SAP and Oracle	Approva and Security Weaver
Financial Risk Management	SAS and SAP	Algorithmics (Operational risk management has become a common component of the EGRC platform)
Financial Analytics	Cognos, SAP and Oracle	ACL and Oversight Systems
Spreadsheet Control	None	Compassoft, Prodiance and ClusterSeven

Source: Gartner (April 2008)

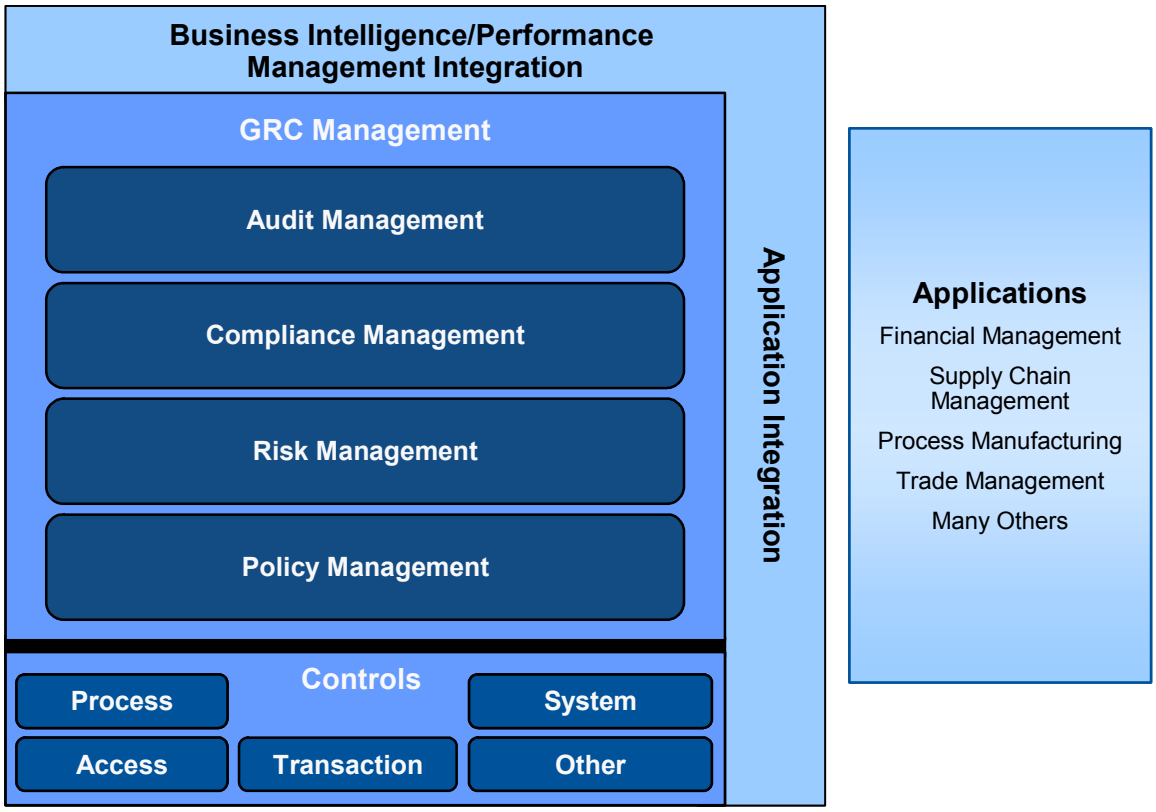
Financial governance offerings (see "Financial Governance Will Emerge to Enhance Financial Controls and Regulatory Reporting") will be targeted directly at the needs of the CFO and finance function, and will contain the following functional areas:

- Financial consolidation — Typically found in CPM suites, these applications enable organizations to reconcile, consolidate, summarize and aggregate financial data based on different accounting standards and federal regulations across multiple legal entities. They also provide reporting tools to support the production of financial statements that represent the overall financial performance of the organization.
- Intercompany transaction management — These are post-ERP consolidation applications, ensuring that interentity transactions are accurate and meet approval, often at the voucher level.

- Reconciliation management — This set of applications ensures that monthly routine account reconciliations are managed and that exceptions are highlighted and handled.
- Financial controls and compliance — As required by SOX, these applications, often delivered as part of an EGRC platform, document and assess financial management controls, and communicate their status across the enterprise.
- Financial close management — This set of applications ensures that the last mile of finance is managed and that all close activities are completed.
- Access and segregation of duties controls — These applications ensure that in transactional and reporting processes there is control over who has access to, contributes to and approves financial processes.
- Financial risk management — These solutions project an organization's tolerance for financial risk, given a series of parameters. This area is not well-served, but solutions targeted at the banking industry should emerge for other vertical industries during the next three to five years.
- Financial analytics — These solutions are used to understand in-period and period-to-period analysis of financial information. This would include a drill down into transactional data to understand varying results. Solution providers in this area include SAP, Cognos, Oracle and The GL Company.
- Spreadsheet control — These solutions ensure the control and auditability of user-defined applications, most notably spreadsheets, critical to financial management and reporting.

As compliance, risk management and financial governance increase the demands for IT support, software vendors and some enterprises are laying the foundation for an integrated EGRC architecture (see Figure 4).

Figure 4. GRC Reference Technology Architecture



Source: Gartner (April 2008)

This architecture will enable the elimination of some process controls because equivalent system controls will be inherent in the evolving architecture. Enterprises will be capable of eliminating numerous compliance-specific applications for audit, disclosure and financial controls, because financial applications will incorporate and support the same functionality. However, spending on point solutions for targeted compliance and risk management needs will continue. A December 2007 Gartner report found that enterprises will spend $566.5 million on finance and audit GRC software solutions in 2008, growing at 20.3% annually to $893.1 million in 2011.

3.0 The Organizational Impact

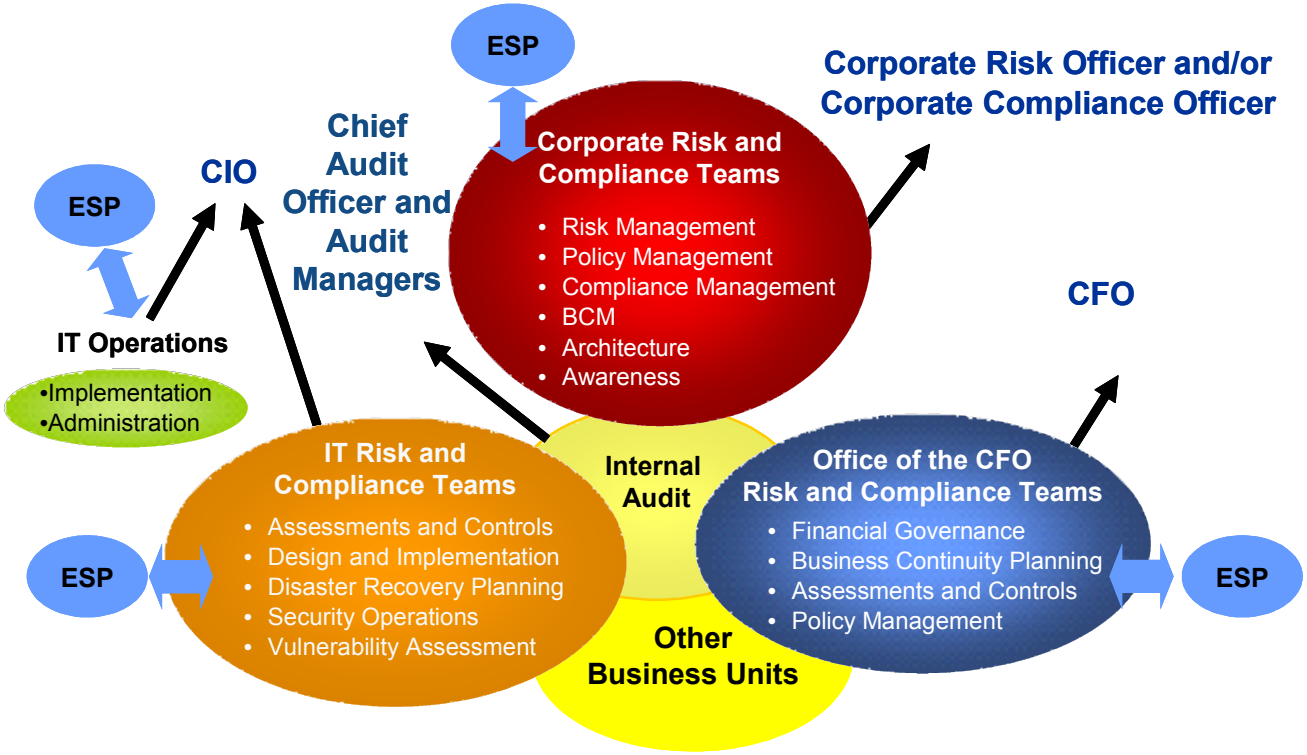
Most enterprises are still organizationally, functionally and technically disaggregated, which can impede business success and make it harder to comply with governmental regulations. As evidence, the finance department often obtains solutions without the involvement of IT, frequently creating a difficult position for the IT department as it tries to exercise control over the application portfolio. This tide must change, and the IT and finance areas, as well as other organizations affected by regulations, must work to improve cooperation.

As organizations begin taking a more holistic approach to GRC management and financial governance, stronger linkages are emerging among compliance, risk management, performance management and corporate business strategy, which, in turn, are developing better alignment of people, processes and technologies. At a minimum, most enterprises that take a top-down, risk-oriented approach to SOX compliance have found that this approach requires better coordination across business entities and corporate functions. The increased coordination has enabled many

enterprises to establish a comprehensive compliance and risk management program with a common set of controls objectives for multiple regulations, policies and standards — thus reducing costs and improving the accountability and alignment of policies, compliance and risk management across the enterprise.

To coordinate GRC activities enterprisewide, a federated organizational model is developing (see Figure 5).

Figure 5. Federated Compliance and Risk Management Organizations



Source: Gartner (April 2008)

Most GRC activities will be embedded in individual business units. Guiding GRC efforts across the enterprise is a council of executive leaders, including the CFO, chief compliance officer, chief risk officer, COO and chief audit officer or their equivalents. An enterprise working group or committee that includes IT compliance and risk managers and their peers in other business units ensures that risk management and compliance activities support the governance and policy objectives established at the senior executive level. These organizational activities can be replicated at the individual entity level for large enterprises. Notably, this level of coordinated action, to be effective, is supported through an EGRC platform.

Many enterprises already have this model, but it will become more prevalent, even in more-centralized organizations, because of the need to:

- Embed business unit compliance and risk management activities in business and IT processes and to align them with enterprise risk management functions
- Emphasize that enterprise risk management encompasses much more than just financial management, internal audit and IT

The level to which this will take place (hence the actual organizational structures, titles and so on) will differ by organization and will be influenced by factors such as:

- Corporate culture and tolerance for overcoming silos
- The level to which segregation of duties is deemed important
- The risk appetite of individual entities and the enterprise as a whole
- The maturity of general risk management practices in each entity

The effectiveness of this model is closely linked to:

- Effective governance, especially a clear understanding of respective accountabilities
- Maturity of "matrix" management capabilities
- Maturity of compliance and risk management processes

4.0 The SOX Knock-On Effect

SOX has a broader impact than just CFOs of enterprises regulated by the SEC. Despite initial resistance in Europe and that SOX-like directives have a less-punitive impact outside the U.S., the auditing standards set by U.S. regulators are spreading internationally and to nonpublic companies. The SOX knock-on effect extends the market beyond companies regulated by the SEC for the following reasons:

- Other countries (notably Canada, Japan and those in the European Union) are establishing SOX-like rules that require internal-control audits and effective risk management programs.
- New international accounting standards are harmonizing accounting practices worldwide. The U.S. is considering replacing generally accepted accounting principles (GAAP) with those of the International Financial Reporting Standards. The SEC is considering making it an option, and some experts believe that it may even become mandatory, meaning a major re-education process for accountants. Although one global standard should simplify the world of accounting, many in the field fear that replacing

U.S. GAAP with international accounting standards could become a solution that ends up more complicated than the problem.

- Auditors are raising corporate governance standards in companies, nonprofit agencies and institutions that are not required to report under SOX regulations.
- Regulators are extending SOX-like governance standards to other regulated markets, such as insurance, banking, brokerages and mutual funds.
- Regulators worldwide continue to be under public scrutiny because of high-profile incidents and perceived inefficiencies of regulatory bodies.
- With an emphasis on public accountability and transparency, some governments are extending new corporate governance standards to their agencies and state-owned corporations.
- Enterprises are pushing SOX-like standards to partners in their extended supply and value chains.
- Nonaccelerated filers to the SEC, companies with a market capitalization of $75 million or less, which have seen numerous deadline extensions, will begin to report under SOX section 404 in 2009 or 2010, depending on whether a proposed extension is adopted.

No matter where an enterprise is located, regardless of whether it is a public or private entity, there is some knock-on effect from SOX, and IT professionals supporting the office of the CFO will be affected. Therefore, it is critical that firms establish programs to continuously monitor regulations and their potential impacts on business processes. In this type of initiative, firms must include the evaluation of technology and how IT can be leveraged to improve compliance and governance efforts.

RECOMMENDED READING

Financial Governance

"Criteria for Selecting Financial Consolidation Solutions"

"Financial Governance Will Emerge to Enhance Financial Controls and Regulatory Reporting"

"Taking a Holistic Approach to the Last Mile of the Financial Close"

"Using CPM and BI to Improve Compliance Initiatives"

Regulatory Guidance and Best Practices

"Best Practices on How to Organize for Sustainable Compliance"

"Gartner for IT Leaders Overview: The IT Compliance Professional"

"New Deadlines Offer SOX Relief to Small-Cap and Startup Firms"

"New SOX Guidance Can Help Cut Audit Costs"

"PCAOB Release No. 2007-005, May 24, 2007"

"Securities and Exchange Commission, 17 CFR Part 241, [Release Nos. 33-8810; 34-55929; FR-77; File No. S7-24-06"

"SOX and 'EuroSOX' Are as Similar as They Are Different"

"Tutorial on How to Move Beyond Security Awareness to Create a Risk-Conscious Culture"

GRC Technology and Markets

"Dataquest Insight: The Finance and Audit GRC Software Markets Are Evolving in Support of Broader GRC Management"

"Hype Cycle for Regulations and Related Standards, 2007"

"MarketScope for Spreadsheet Control Products, 2008"

"The Enterprise Governance Risk and Compliance Platform Defined"

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner