

The ROI of SOX

SOX COMPLIANCE INVESTMENTS CAN BOOST YOUR BOTTOM LINE

BY ROBERT PUTRUS, PE, CMC

While Sarbanes-Oxley compliance costs can vary depending on a company's revenue, operational reach and ownership structure, many businesses have experienced a multifold return on investment, ranging from the introduction of new initiatives to the implementation of improved business processes.

Businesses can boost their bottom line if they approach SOX compliance as an opportunity to improve the business' management, as well as to reduce the costs of operations and internal audits.

SOX COMPLIANCE

In general, SOX compliance investments can be classified into one or more of the following:

- Information Technology—investments in infrastructure, such as networks, system management and software;
- Business Controls—investments in enterprise resource planning, supply chain management, customer relationship management, etc.; and
- Company Policy and Management—management decisions regarding the centralization or decentralization of the business' processes; mapping management accountability into processes; and improvements to corporate governance.

This article focuses on the quantification of SOX compliance benefits and the ROI of IT and business controls initiatives, the combination of which can provide controls to prevent fraud, misuse or loss of financial data transaction; enable speedy detection if and when such problems occur; and allow preventative action to be taken to limit and mitigate the effects of the problems.

IT CONTROLS

There are four basic general controls within the IT initiative as stated by Control Objectives for Information and related Technology:

IT planning and governance—includes information systems strategic plan; the IT risk management process; compliance and regulatory management; and IT policies, procedures and standards.

Computer systems management and operations—controls over the definition,

acquisition, installation, configuration, integration and maintenance of the IT infrastructure. This will include service level management; management of third-party services; system availability; problem and incident management; and facilities management.

Program or application development and change controls—controls over the acquisition and implementation of new applications and the maintenance of existing applications. The risks are controlled through the development and compliance to system development and quality assurance methodology. The methodology provides guidelines for the system design and implementation, documentation, testing, approvals, project management, etc. New releases of software will fall under application maintenance and ongoing change management.

Computer security and access controls—control activities in the design and implementation of secure passwords, internet firewalls and data encryption. Applications will provide access privilege only to authorized users as defined and approved by company management.

BUSINESS CONTROLS

Business controls ensure that the values on the financial income statement and balance sheets are accurate and reliable. These controls are provided through enterprise resource planning, supply chain management and customer relationship management applications. They also could be referred to as "application controls," where transactions are initialized, authorized, implemented, reported and validated.

For example, accounts payable or receivable are performed through the transactional means and recorded in the accounting general ledger system and financial statements.

Both IT and business controls are governed by documented policies and procedures and segregation of duty. When



application controls do not follow the documented procedure, and when the same person initiates and approves the same transaction, such as entering invoice information in the system, approving the invoice, changing vendor information in the system and issuing check for payment, this is a *segregation of duty* violation. As a result, the control is deemed ineffective.

IMPROVING THROUGH SOX

IT and business controls can lead to various types of business opportunities, including:

- **Financial Improvements.** This can be realized, for example, by implementing an ERP application that automates controls and standardizes process. For example, the ERP software can be configured to enable the company to identify and apply control rules that automate the segregation of duty rules to prevent potential violations.

- **Control Improvements.** This could be realized by implementing Standards on Auditing Standard 70, segregation of duty, etc. For example, SAS 70, "Service Organizations," provides auditors with guidance in evaluating service organizations in the context of a financial statement audit. Service organizations that successfully complete an SAS 70 audit have been through an in-depth

Sarbanes-Oxley Business Model

GOAL: REDUCING MATERIAL MISSTATEMENTS, ERRORS & FRAUD

COMPLIANCE OBJECTIVES	RAPID DISCLOSURE	INTERNAL CONTROLS & PROCEDURES	ACCELERATED REPORTING	REDUCE INTERNAL AUDIT COSTS
CRITICAL SUCCESS FACTORS	SEEKING ACCURACY	SEEKING TIMELINESS	ACHIEVING QUALITY	ORGANIZATION TRANSPARENCY
CORE PROCESSES	MANAGING FINANCE & ACCOUNTING	MANAGING SUPPLY CHAIN	MANAGING RESOURCES	MANAGING INFORMATION TECHNOLOGY
BUSINESS CHALLENGES	ON-GOING CONTROL	PROCESS STANDARDIZATION	PROCEDURE AUTOMATION	STREAMLINING
BUSINESS ENABLERS	INTEGRATING MULTIPLE SOURCES	DELIVERY IN REAL-TIME	TIMELY, DETAILED REPORTING	REDESIGNING ACCOUNTABILITY

audit of their control activities, including controls over information technology and related processes.

There are two types of SAS 70: Type I and Type II Reports. In Type II Reports, auditors provide an opinion on whether or not the controls that were tested were operating with sufficient effectiveness to provide reasonable—but not absolute—assurance that the control objectives were achieved during the period specified. These are the reports auditors seem to be accepting

Also, segregation of duty is a control that reduces risk by separating the custody of assets from accounting personnel, sepa-

rating the authorization of transactions from custody of related assets, and separating operational responsibilities from record keeping responsibilities.

- **Productivity Improvements.** This could be realized by implementing standard processes; centralizing processes, such as accounts payable or receivable; or aligning IT initiatives with company objectives, such as supply chain management implementation.

SOX AND SOURCES OF ROI
SOX presents many ROI opportunities for each business segment and core process.

For example, in Exhibit 1, under “Business Enabler,” if a feature like “timely, detailed reporting” is automated, say through the development and distribution rules of such reports through the use of enterprise report writer applications, it will impact the report’s timeliness and transparency, as well as its delivery to proper staff throughout the organization. Ultimately, it will lead to rapid disclosure and accelerated reporting, which will result in greater operational effectiveness.

The same logic applies when automated controls are realized by implementing an ERP application, ensuring standardization

A Preferred SBA Lender

Popular Small Business Capital, is a National SBA lender specializing in financing Real Estate, Business Acquisitions, Equipment, Inventory and Working Capital for small businesses. Our loans range from \$150,000 to over \$5,000,000.

For more information or to discuss a particular deal, contact your local Business Development Officer.

Art Concha - Los Angeles
(562) 622-2785

Tony Im - Sacramento
(916) 515-4179

John Owens - Elk Grove
(916) 714-7241

Jonathan Park - Anaheim
(213) 291-9772

Mark Decius - San Francisco
(415) 206-1800



POPULAR
Small Business CapitalSM

A division of Banco Popular North America

Make
Dreams Happen

www.popularsmallbiz.com





The New Face of Workers' Comp

Over the last few years, there have been many changes to the California workers' compensation system. And there are more changes to come.

These changes can provide big opportunities for your business owner clients. Workers' comp is one of their big expense items. Now, cash flow and earnings can be improved because rates have been reduced by nearly 50%. New rules give employers the control over claims they wanted, but now it's up to them to select an insurance carrier that knows how to fight fraud and has the determination to win.

Those who would cheat the system and undo the positive changes have not gone away. Do you or your clients know what the new face of workers' comp fraud looks like?

We do. We're *Employers Direct Insurance Company, California's Workers' Comp Specialist*, and we're committed to protecting your clients by stopping workers' comp fraud dead in its tracks!



CALIFORNIA'S WORKERS' COMP SPECIALIST®

We're a direct writer not available through agents or brokers. But you or your clients can call us anytime!

Call 866-421-8500 or visit www.employersdirect.com

Employers Direct Insurance Company is a proud member of the Workers' Compensation Action Network, a grassroots organization of over 1,000 California businesses dedicated to promoting workers' compensation reform.

and an active control status throughout the enterprise. Also, this will impact the enterprise model (Exhibit 1), and can reduce the internal audit cost by ensuring the implementation of internal controls and procedures.

Preventative controls are the preferred status of controls and are recognized when the controls are automated, and will drastically reduce the audit cost by reducing the selected sample size for testing and expedited completion of the tasks.

THE ROI METHODOLOGY

The following methodology to quantify the returns and the realized benefits for the calculation of the ROI is based on non-traditional accounting techniques. ROI justification is a traditional accounting method based on a Discounted Cash Flow analysis. However, this fails to account for and quantify the intangible benefits of compliance.

Where does that leave us? SOX compliance investments in IT and automation will be justified in non-traditional accounting methods. For example, to quantify the intangible benefits and rationalize the ROI of SOX compliance using non-financial methodology, such as the Analytic Hierarchy Process techniques. The following is a summary of the steps:

BUILDING THE MODEL

The proposed process to build the SOX compliance model (Exhibit 1) is based on management workshop setting; rule of collaboration/consensus; development of hierarchical model; and implementation of the AHP techniques.

Management Workshop Setting: A forum where a company structure is represented as the official entity of each of the operating units. The company staff that carries the credibility of understanding and discretion to propose, support and implement the changes represents the units. These are the people who should participate in the workshop to build the SOX compliance model and carry out the ROI analysis.


Collaboration: All individuals participating in the management workshop must agree to a collaborative approach in the design, prioritization and implementation of the AHP process.

Development of Company SOX Compliance Model: The SOX compliance model is a representation of the company that describes the business, management and the intra-relationship of its entities. Exhibit 1 is an example, which is developed of six hierarchical layers: Ultimate Goal; Compliance Objectives; Critical Success Factors; Core Processes, Business Challenges; and Business Enablers.

Each layer is defined by distinct components and could include an unlimited number of attributes. The components of each layer are linked to those of the layer above and below that are governed by the AHP technique. The value of impact are quantified and represented by each of the stated company "Business Enablers." All layers are linked in hierarchical form and each element in the business model can be expressed in a quantifiable fashion by all the elements in the layer below.

Accepting the AHP Tools: The tool used in a management workshop forum is easy to use and establishes the links between different layers of the model attributes using a reliable ranking/prioritization technique of AHP. Download more information at <http://sigma.poligran.edu.co/politecnico/apoyo/Decisiones/curso/Interfaces.pdf>.

CONCLUSION

SOX 404 compliance opens the door for companies to evaluate their processes and procedures, and to measure their gap with the best practices. Doing so will help companies improve their business practices—and their bottom line. 

Robert Putrus, PE, CMC is the principal of Southern California-based Robert Putrus Consulting, an information technology and risk consulting firm. You can reach him at robertputrus@therobertsglobal.com.