SOX, ERP, and BPM

A Trifecta That Can Make Your Business Run Better

By Kenton B. Walker

In 2002, Congress passed the Sarbanes-Oxley Act (SOX) to improve transparency and accountability in business processes and corporate accounting that should lead to increased confidence in public markets. One key provision of this law, Section 404, has proved to be particularly difficult for companies, especially those that didn't have good internal controls, processes, and procedures already in place. As you know, Section 404 spells out the requirements for internal controls documentation, assessment, and testing activities that govern the creation of financial reports. The law requires that the management of publicly traded companies attest to the effectiveness of internal controls in each annual report they file with the Securities & Exchange Commission (SEC).

SOX compliance is about financial reporting, focusing on establishing good business practices, and ensuring proper controls are in place to identify potential areas of concern for management. But some executives also have been viewing and using it as an opportunity to streamline and improve business processes, improve efficiency, and increase competitiveness. In fact, companies that are having the most success began their compliance route by asking "How would we implement a corporate performance measurement and financial data accuracy initiative in the absence of SOX?" Regardless of the approach chosen, companies have found that most solutions have relied heavily on their information systems. Enterprise resource planning (ERP) systems and business process management (BPM) tools are two established and valuable resources that together are helping companies comply with SOX and make the business run better.

ERP SUPPORT

Most organizations have been using ERP systems for years. ERP solution providers originally designed their products to achieve automation across multiple departments in organizations, primarily to aid management of manufacturing and distribution processes. These systems offer a framework for organizations to work effectively and efficiently and provide for the establishment and management of standardized processes for raw materials, inventory, order entry, and distribution activities.

At the same time, ERP can help companies improve the systems environment, streamline business processes, and comply with SOX. Principally, ERP goes a long way toward eliminating fragmented and incompatible systems. It also provides support for SOX compliance in several important areas, including accounting, internal controls, and merging the physical and financial supply chains. Yet many ERP systems are out of date or still too decentralized to assist with Section 404 compliance, which has led to increased IT spending to support SOX compliance initiatives. In addition, there are some Section 404 compliance requirements that ERP alone doesn't satisfy.

Support for Accounting

Accounting is experiencing some important benefits of ERP: Duplicate files and redundant data entry are no longer necessary. Accountants can simulate product costs and analyze impacts of changes in labor rates, material costs, overhead rates, bills of materials, and product routings. Customer invoices may be based on actual shipments without duplicate data entry, which helps speed invoice processing. Matching of records for payment processing can be completely automated. As products progress through manufacturing, an ERP system can automatically record transactions and update the general ledger. This provides a complete audit trail from source documents to account balances, ensures accurate and current financial information, and permits tracking of actual activity against the budget.

ERP performs period closings quickly, eliminates or reduces clerical accounting errors, provides timelier financial reports, and permits customization of financial reports to meet the needs of individual managers. Financial projections can be prepared based on detailed information contained within a common database, thus eliminating inconsistencies that happen with multiple corporate information systems. Cash planning can account for current and projected orders, purchases, receivables, and payables.

ERP vendors are constantly introducing new reporting and consolidation tools to make financial processes more efficient and to assist with compliance. In an effort to improve external disclosures, they're developing software for more informed, timely, and comprehensive internal reporting. These capabilities give managers better visibility into current operations and for preparing forecasts. This provides the ability to create performance "watchdogs" who serve as an early-warning system for important corporate performance metrics.

Support for Internal Controls

ERP systems incorporate control features that support SOX and other types of compliance. Information system controls can be segregated into three levels: organization, which relate to the entire organization and structure; entity, which address a business unit or division; and process, which are concerned with documentation and control over a specific business process. Process-level controls are further divided into general IT controls, application integration controls, and data ownership controls. There are also process-level controls that specifically support compliance.

General IT controls include security administration, data management, problem management, asset management, and change management. ERP systems can support security management controls by utilizing tools delivered for establishing security roles, user IDs, passwords, and specific module access. Examples of data management controls include limiting the ability of individuals to enter or change data and protecting data using a secure

Completion of the processes in an ERP system in accordance with the documentation demonstrates consistency and compliance to external auditors.

environment with regular data backups. Problem management controls include separate testing and production environments, standardized problem resolution procedures, and effective troubleshooting practices. Asset management controls include records of each IT asset's location and use, routine update and maintenance activities, and personnel access to system hardware. Change management controls include proper procedures and documentation for authorizing system changes and a separate quality assurance function to move changes into production. Though not all of these general controls are contained within all ERP application software products, they are part of recognized ERP implementation best practices. A weakness in general controls can affect the integrity of the entire system, and external auditors might consider such a weakness to be material.

Application integration controls apply to multiple applications that work together to process financial data and produce financial reports. ERP systems reinforce integrated controls by employing standardized, cross-functional, and industry best practices. Documentation of business processes demonstrates the internal control structure by identifying sources and uses of data, proper separation of duties, and necessary approvals. Completion of the processes in an ERP system in accordance with the documentation demonstrates consistency and compliance to external auditors.

Application and data ownership controls are concerned with ownership of the process and associated data. Controls in this area are specific to software modules or functions within those modules. Examples include granular security access, automated business processes, utilizing workflow for evidence of transaction reviews and approvals, and maintenance of transactional audit trails. ERP provides good controls in this area.

Support for Merging Physical and Financial Supply Chains

As you know, SOX requires senior executives to be personally responsible for reporting the impacts of supply chain delays on inventory valuations and company revenues. To meet these requirements, it's important to unite the physical and financial sides of supply chain management. Reports from supply chain executives suggest that they're concerned about compliance but have been incorporating new financial reporting requirements into larger process improvement initiatives.

The biggest concern is with contract compliance. Some prominent ERP solution providers have introduced global trade management (GTM) modules to improve ERP effectiveness for managing important supply chain business processes. This software provides improved information visibility, and managers are able to make better decisions about how to lower inventory, reduce the number of days outstanding for accounts receivable, and shorten the cash-to-cash cycle.

Some key features of GTM products include:

- A single repository of all contracts;
- Execution, capture, and management of purchase order transactions and related transactions such as travel and entertainment;
- Execution, matching, payment, dispute resolution, and analysis of vendor invoices against contracts, authorized transactions, receiving, and performance information;
- Capture, classification, and analysis of spending; and
- Tracking of key performance indicators against agreements.

Supply managers gain better visibility and control over spending, inventory, and outsourcing decisions with these products. Business benefits include: (1) transparent trade processes, (2) standardized and automated processes that should require fewer steps and execute faster, (3) improved profitability analysis on deals because of automatic profit and loss calculations based on actual and estimated expenses and automatic settlement of expenses when received, (4) more complete cost assignment as a result of expense management features that permit early application, and (5) better control over risks from integration with financial applications that allow users to monitor cash, inventory, and hedging activities.

Payroll shows many good examples of how BPM can effectively monitor processes to achieve SOX compliance and help your business run better.

Compliance Gaps in ERP

ERP systems generally aren't sufficient to provide for complete compliance with SOX. At the core, they're designed to meet transactional needs. While these systems capture most of the needed information, there are often weaknesses in managers' ability to use it. The information isn't easily accessible in a meaningful format, and it's difficult to relate across departments and organizations. Some systems may not retain necessary histories in areas such as approvals, master record changes, and significant financial inputs. ERP systems typically don't document policies and procedures, although some vendors are adding this capability. Another area of concern is mechanisms for alerts to detect irregular business patterns.

The largest compliance gap is the inability to provide a truly consolidated view of an organization. Early ERP products didn't extend to areas such as sales, marketing, services, noninventory, nonorder transactions, and external partners and vendors. They didn't tie in customer relationship management (CRM) capabilities that would allow companies to collect customer-specific information, nor did they work with the development of websites or portals for customer service orders. These solutions also couldn't handle document management, such as cataloging contracts and purchase orders. As the idea of the extended enterprise emerged, people began asking questions about how to effectively integrate members of the value chain. The answers to these questions led to the development of business process management technology.

BPM SOFTWARE SUPPORT

BPM provides visibility and control over all portions of a transaction or information request that spans multiple applications, functions, and individuals in one or more organizations. This software can help companies identify processes that need to be automated, automate workflow, monitor and enforce business rules for human and automated processes, and integrate the IT infrastructure with enterprise application integration (EAI) tools. BPM software does this by extracting data from all of a company's business applications and either tracking how individuals use information to perform a task so that you can map a business process or shepherding the data through a series of tasks to ensure that people follow a prescribed business process.

BPM workflow products automate portions of a process and direct tasks to be performed by particular individuals to ensure that the process is followed. Processes include everything from routine activities, such as work orders, customer interactions, and payroll processing, to mission-critical processes, such as payment remittance, billing, product development, and logistics. A workflow BPM system will prevent a sales representative from opening a new account if one already exists, stop a payment that doesn't have proper authorization, require a call center worker to verify the identity of a customer, and necessitate a series of predetermined steps to follow when hiring a new employee. In order to implement BPM workflow, the people who use the system must prepare a detailed map of the processes that they want the system to follow and enforce, which means the new system will be only as good as the process design.

BPM serves as a process monitor much as efficiency experts from decades ago observed and recorded manual process activities. For example, BPM might track an order from the time it's placed until it's shipped. As a result, a company might discover unexpected delays between steps in the process. Monitoring software may also be used to issue alerts when an employee doesn't follow the correct steps in a process.

Finally, business process management helps integrate the information contained in separate business applications.

Capabilities that Support Compliance

BPM software automates the process of evaluating old controls and updating documentation of new controls. When a company changes a business process, the software requires the process owner to simultaneously evaluate the design of controls, evaluate their relevance, and make appropriate changes. The software also captures any

changes, eliminating the need to update a separate record of control descriptions. For example, when an employee checks vendor invoices for payment, he or she must follow particular steps that are documented electronically. In an electronic environment, the system restricts processing options to ensure that the approved procedures are followed. The process owner can't introduce a new document, such as a purchase order, into the system without defining how the use of the document will be controlled. As a result, there's no time lag between the introduction of a business process and the implementation or change of control. The risk that control deficiencies will evolve in a changing business environment is greatly reduced.

Payroll shows many good examples of how BPM can effectively monitor processes to achieve SOX compliance and help your business run better. For instance, someone in HR must authorize payroll changes, and the head of the department in which an employee works must approve all salary changes. Routine, highly structured activities are another example. Payroll personnel should process all payroll transactions according to management's criteria, but these criteria must be clearly documented. Things that can go wrong include payroll transactions not being properly authorized and payroll balances not being substantiated or evaluated appropriately. In both cases, a company must to able to show that there are controls in place to cover these risks.

Assume that each pay period a payroll clerk must review and reconcile budgeted vs. actual payroll. If the difference is greater than 2%, the clerk must report the discrepancy and document the reason. If the difference is 4% or greater, it must be relayed to the department manager for an explanation and then to the finance director for review. At each stage, participants in the process can record any unresolved issues. The process continues until all issues are resolved and steps in the process are approved by the predetermined authority. Automated alerts tell the payroll clerk when it's time to reconcile payroll, route information for approvals, identify the location of the payroll reconciliation within the approval process, document issues, record the disposition of any issues noted in the process, and provide evidence to fulfill the requirements of SOX.

Providing evidence of these internal controls could take months in most ERP systems, and, if the processes or people change, reconfiguring the system may be expensive. BPM software can provide self-documenting and secure audit trails. Similar internal control functions are available for reconciliation and approval of general ledger entries, purchase-to-pay processes, and order-to-cash, including discount approvals, customer signatures, credit approvals, and contract approvals.

There are a number of BPM functions that management should look for in any software product:

- Documents and enforces business rules and internal controls for business processes across information systems applications and multiple lines of business.
- Develops a complete audit trail for corporate processes so auditors can immediately retrieve any transaction, see its routing and approval path, and review supporting documents and data.
- Monitors business processes in real time and delivers system-wide reporting capabilities to provide visibility into business processes and enable individuals to identify weaknesses or deficiencies in process controls.
- Provides real-time visibility into information content at every stage of a business process.
- Offers flexibility to address changing regulatory requirements, other compliance initiatives, and business management tools.
- Features a highly scalable, fault-tolerant, open architecture that accommodates growth in personnel, processes, and information across the enterprise and spans the gaps between departments and lines of business.
- Supports Lightweight Directory Access Protocol (LDAP), single sign-on, and digital signatures to meet SOX guidelines for nonrepudiation.
- Offers a secure, client-server environment to improve security and privacy of transactions to meet SOX requirements for acceptable data security.

SOX AS A CATALYST

For Cultural Change

SOX compliance initiatives have been the catalyst for significant organizational changes. The first change is to make organizations "informationally transparent." ERP systems provide the bulk of transaction information transparency, and BPM provides business process transparency. Permitting wide access to information supports an ethical business environment and drives organizations to improve performance because more individuals are able to view process transactions and activities, the interfaces between organizational boundaries, and performance of process activities. New and unbiased perspectives on organizational conduct are possible as individuals previously excluded from viewing informa-

tion acquire access. Inadequate controls, loose audit trails, outdated document management strategies, and resistance to change are identified, and corrective action can be taken on a timely basis. Organizations become more nimble, relevant, and responsive to internal and external customers.

For IT Upgrades

The upshot of SOX for information systems is that corporate governance issues are encouraging companies to purchase or upgrade ERP systems. Companies that previously couldn't make a business case for ERP can do so now. They are gaining unparalleled business awareness through ERP and a SOX audit as an achievement standard. Firms need to determine if their current systems retain historical information on financial inputs, master record changes, and authorizations/approvals. From this information, an organization can detect unusual business patterns and investigate any problems. Companies should also evaluate data storage methods to determine such things as how records can be deleted, how secure is data, who can access data, and, of those who can, how many have a business purpose. Finally, compliance necessitates that companies assess mechanisms for alerts that would detect irregular business patterns. These alerts range from a portal dashboard to the ability to obtain information from control reports.

To Uncover and Repair ERP System Weaknesses

Being aware of an information system's weaknesses is as important as knowing its strengths. Shortcomings may be inherent to the system, the result of poor implementation, or simply stem from management's failure to fully utilize existing system capabilities. Compliance initiatives can provide an important barometer of the state of information system and business practices. Even smaller firms that use ERP and that aren't required to comply with SOX need proper business controls in place to identify weak spots.

Companies that operate an ERP system are required to have an audit of the system for SOX compliance. Before accounting/finance and IT managers can leverage ERP as a compliance tool, they must evaluate the status of the system's "switches" and the internal controls corresponding to each one in every functional area supported by the ERP package. There are many examples of organizations that spent millions of dollars on ERP but didn't experience its value. After examining the implementation, managers discovered that problems weren't a result of the software failing to perform as advertised but of failure to enable control mechanisms (the switches were turned "off") during the implementation, set-up, and monitoring phases. In order to lower the cost and speed up the implementations, some companies didn't take the time to fully enable their systems. System implementers didn't turn on some of the internal controls now needed for compliance efforts.

One example involves restrictions placed on access to specific modules of the ERP system. In some organizations, employees outside accounts payable can make entries to the AP module. Access wasn't sufficiently restricted during the implementation process and may not be sufficiently documented to satisfy external auditors that the company complies with Section 404. Another example is workflow controls. Many ERP systems can be used to define the level at which a potential accounts receivable write-off must receive approval. If the control "switches" are set properly, write-offs that exceed the threshold will be automatically routed to the appropriate finance manager or controller.

For many years, companies used spreadsheets to manage processes, but spreadsheets don't provide process controls, an audit trail, or reporting required to constitute evidence under SOX. Many companies have tried to implement or reconfigure their ERP systems to satisfy SOX requirements, but these systems are complex, difficult to configure, expensive to use and maintain, and are often unsuitable for this purpose. BPM can be valuable here because of its ability to consolidate data from multiple information systems.

Companies also must audit the process for approving financial statements and collecting records, and they must demonstrate that the process is followed in a procedural audit above and beyond the financial audit. In other words, a firm must prove that it's doing business in the way it says it does. ERP packages usually don't document policies and procedures, although this is changing in many new product offerings. For companies that use ERP and BPM applications, this step is easy because together these complementary systems can create, execute, and monitor workflows and generate an audit trail.

In addition, "internal controls manager" modules document risks associated with business processes and help companies mitigate those risks. These capabilities generally duplicate the Section 404-specific applications that the major accounting firms, document and risk management vendors, and finance and accounting consultants offer.

To Improve Communications between Functional, Finance, and IT Personnel

Compliance efforts require extensive communications and cooperation among three important groups: (1) individuals with security experience and IT architects with practical experience in identity and access management processes and technology; (2) audit, finance, legal, and compliance professionals who are responsible for defining, planning, executing, and testing for SOX compliance; and (3) functional personnel who use the system. IT departments and business and financial processes are usually intertwined, so an internal controls assessment automatically becomes an IT audit at the same time.

Business processes are the thread that binds functional activities and technology processes. From a technology perspective, the business processes that are of particular relevance to Section 404 compliance include:

- Data input, financial statement preparation, and financial consolidation.
- Purchase requisition to vendor payment.
- Sales order to customer remittance.
- Asset acquisition to disposal/write-off.
- Project initiation to revenue recognition.
- Intercompany transaction processing.
- Currency translation in financial reporting.

Compliance requirements necessitate communications and technology solutions that will provide information such as:

- The source of data that will be presented in reports.
- Identification information that binds an individual who entered, changed, or modified data to a financial report.
- The original classification of information.
- Assurance that tampering hasn't occurred.
- Processes the information has gone through to reach the report.
- Roles and authorities of individuals who have had access to the information.

THREE PHASES OF COMPLIANCE

Compliance initiatives generally move through three phases: (1) check-off, (2) acceptance of the directives within the law, and (3) attempts to leverage compliance efforts into benefits beyond what the law requires. The question concerning phase three is "How far?"

A three-stage approach can help answer this question. First, audit the IT infrastructure with the ERP system as the primary focus because ERP is the primary transactional source for financial disclosures. Firms should examine how much of the system is implemented, how it was implemented, and if it's being used properly. Second, determine how any past or contemplated investments in compliance products complement the IT strategy. If your company has invested in BPM software, should it be linked with the ERP product? If there are multiple ERP products and legacy systems, should these systems be further consolidated? These are decisions that require the cooperation of the CFO, CIO, and other C-level executives. Finally, identify additional benefits that compliance efforts can deliver. An effective ERP/BPM solution will help an organization achieve a substantial return on investment and improve its business processes and procedures while complying with SOX Section 404 requirements. The trifecta delivers. ■

Kenton B. Walker, Ph.D., is a professor of accounting at the University of Wyoming. You can reach him at (307) 766-3154 or kbwalk@uwyo.edu.