ASAC 2007
Ottawa, Ontario

Vinod Kumar
Raili Pollanen
Bharat Maheshwari
Eric Sprott School of Business
Carleton University

ENHANCING ERP SYSTEMS FOR SOX COMPLIANCE: KEY ISSUES AND CHALLENGES

The Sarbanes-Oxley Act (SOX) introduced in 2002 by the United States government as a response to some blatant corporate frauds, such as Enron, has brought about widespread changes in the way publicly listed firms manage and report performance. While this legislation has put a serious mandate and responsibility on organizations and its managers to improve their corporate governance, risk management, and performance reporting processes, corporate initiatives to comply with SOX also require significant enhancements to ERP systems. ERP systems provide the primary means and foundations for implementing internal controls and improving business processes, which are critical for complying with SOX regulations. In this paper, we analyze the challenges faced by firms in enhancing their ERP systems to comply with the new legislative requirements imposed by SOX.

1. Introduction

Several empirical studies of ERP adopting firms point out that implementation of ERP software is just the beginning of an organization's ERP program and that firms need to continuously enhance their business processes and ERP systems in order to achieve desired organizational performance objectives (Markus and Tanis, 2000; Davenport 2000). In the last few years, a new urgency to this need has been provided by the Public Company Accounting Reform and Investor Protection Act of 2002. This act, which is popularly known as the Sarbanes-Oxley (SOX) Act after Senator Paul Sarbanes and Representative Michael Oxley, the two lawmakers responsible for leading the legislation, introduced widespread changes in the way publicly listed firms must manage and report their performance.

The SOX legislation requires top management to certify and report on the adequacy and effectiveness of internal controls over financial reporting. In addition, independent auditors are required to attest to the effectiveness of these controls. The implementation of effective controls has forced firms and their auditors to focus on improving the capabilities of their systems and operational processes, not just controlling and certifying the output of these systems and processes. Firms in the post-SOX regulative environment need to improve their processes, enhance their systems, and adopt effective controls in order to improve the consistency and quality of financial information reported to their stakeholders. Interestingly, the changes introduced by SOX are quite analogous to a paradigm shift observed in quality management in the 1980s, when firms moved from quality control to total quality management (TQM). Some of the key elements of TQM are very similar to those firms need today to improve corporate governance

and financial reporting to comply with the new legislations. Like TQM SOX compliance leads firms to move from a detection based approach to a recommended approach of prevention. SOX compliance initiatives also call for the commitment of leadership (CEO), planning and organization, tools and techniques, education and training, employee involvement, teamwork, measurement and feedback, and culture change.

Compliance with SOX requires all public companies to review their ERP systems, and most companies to enhance their systems to encompass new and diverse information requirements and measures for evaluating the effectiveness of controls and the capability of related processes. ERP systems provide technical tools and solutions for collecting, analyzing, and reporting relevant information for implementing internal controls. As such, ERP systems must be capable of integrating both financial and non-financial information from internal and external sources. However, the implementation of technical systems can be complicated, and often also requires adjustments to organizational structures, processes, norms, and employee skills, which can vary in different environments. In large organizations, such efforts can be further complicated by differences in geographic distance, culture, existing technology and systems, and political and regulatory environment in different countries. Inadequate attention to these factors can pose serious challenges for successful implementation. On the other hand, medium- and small-sized organizations can find it difficult to obtain adequate resources to support these efforts. Nonetheless, little guidance exists to help managers and researchers understand control implementation challenges and to enhance ERP systems for control purposes in today's competitive and global business environment.

In this paper, we analyze key challenges faced by medium-sized and large organizations in enhancing their ERP systems for SOX compliance. The analysis is based on data collected through case studies of four multi-site ERP-adopting organizations, and secondary sources such as magazine and journal articles and websites. The study improves our understanding of major challenges and improvement opportunities organizations face in enhancing their ERP systems for SOX compliance. It provides managers some insight into successful practices and challenges in enhancing ERP systems for this purpose, which, in turn, can contribute to the development of best practices and to organizational effectiveness.

2. Background

SOX Compliance

SOX compliance involves significant changes to various elements, such as the role of managers, external auditors, reporting to external stakeholders, and data quality. Interestingly, compliance with SOX, which can be said to be outcome-oriented legislation, is an ongoing process. The legislation only specifies the outcomes and penalties of not complying, whereas the means and normally accepted standards of compliance have been left for other bodies, such as the Public Company Oversight Board. In the words of John Hagerty at AMR Research, "SOX Compliance is a four-phase project, and phase four lasts forever." Clearly, SOX compliance is an ongoing process for firms, as new knowledge is gathered around effectiveness of compliance initiatives, and best practices evolve. It is also dynamic in nature, as firms may find that its processes, which were compliant this year, may become non-compliant next year, while progress made on non-compliant processes this year can result in their compliance in the next audit.

Kendal (2004) argued that the major requirement of SOX, which make it a high-impact legislation, is the legal responsibility and liability of the Chief Executive Officers (CEOs) and the Chief Financial Officers (CFOs) for:

1) Establishing, evaluation, and monitoring the effectiveness of internal control over financial reporting and disclosure.
2) Designing, establishing, and maintaining 'disclosure controls and procedures' and reporting on the effectiveness of 'disclosure controls and procedures.'
3) Disclosing to the audit committee and external auditor any significant deficiencies and material weaknesses in internal controls for financial reporting and any fraud (material or not) involving anyone having a significant role in those internal controls.
4) Disclosing whether after their most recent evaluation, significant changes occurred that affected internal controls for financial reporting and whether any corrective actions were taken with regard to significant deficiencies and material weaknesses.

The most extensive requirements of SOX, with the broadest implications for ERP systems, are those in Section 404. Section 404 requires senior management (CEOs and CFOs) to establish and maintain adequate internal controls over financial reporting, assess the effectiveness of such controls, and certify and report the conclusions of their assessment. In addition, it requires the company's independent auditors to certify and report on the adequacy of the management's internal control assessment. Although SOX is a US law, all companies who trade on the US stock exchanges and foreign subsidiaries of US companies must also comply with it. In addition, Canadian provincial securities regulators are in the process of implementing similar regulations. Although the proposed Canadian regulations do not require certification by external auditors, they require equal managerial effort in implementing and certifying the effectiveness of internal controls (Canadian Securities Administrators, 2006). Therefore, establishing and maintaining effective internal controls is critical to all Canadian public companies.

In general, internal controls consist of rules, procedures, and processes aimed at ensuring the efficiency and effectiveness of operations, reliability of financial reporting, safeguarding of assets, and compliance with laws and regulations. In addition to maintaining adequate records of all aspects of operations, general internal control mechanisms include the segregation of duties, insuring and bonding employees, restricting access to data and assets, and conducting regular independent reviews. Furthermore, specific operational efficiencies and safeguards can be achieved by using appropriate process controls over various areas of operations, for example, inventory management, production scheduling, quality control, equipment maintenance, and supply chain management. For example, Brown and Nasuti (2005) argued that SOX compliance requires ongoing risk management and that firms must continuously evaluate their operational processes, which drive financial transactions and related risks.

An internal control framework developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO, 1992, 2004) has been used almost exclusively as a foundation for implementing internal controls required by SOX.[1] The framework provides general principles for effective

[1] COSO is a voluntary organization dedicated to improving financial reporting quality. Although the U.S. Securities and Exchange Commission (SEC) and the Public Company Accounting Oversight Board (PCAOB) have suggested the use of the COSO framework for implementing SOX, they do not endorse or require a specific framework. The 2004 framework considers internal controls within a more integrative risk management framework.

internal controls but does not prescribe what should be reported. It identifies five control components: control environment, risk assessment, control activities, information and communication, and monitoring. Control environment includes factors, such as organizational norms, ethical values, staff competencies, and management philosophy and style, which set structures and processes for organizational operations. Risk assessment is necessary to manage risks that can stem from uncertainties in economic, industry, regulatory, and operating environments. Control activities are policies and procedures that help ensure the achievement of organizational objectives, and include approvals, authorizations, verifications, reconciliations, and performance reviews. Information producing and communication activities include collecting, analyzing, reporting, and communicating relevant information to ensure individuals have information necessary for understanding and performing their responsibilities related to internal control. Monitoring consists of processes, activities, and actions by management and supervisors to ensure the quality of internal controls over time and includes both ongoing monitoring and periodic evaluations. Some examples of control mechanisms for each control component are provided in Table 1.

Table 1

Control Components and Objectives

Control Component	Purpose	Examples
Control environment	To set structures and processes for organizational operations	Organizational norms Ethical values Staff competencies Management philosophy and style
Risk assessment	To manage operational and environmental risks	Environmental scanning Risk management frameworks Forecasting models
Control activities	To ensure achievement of organizational objectives	Approvals Authorizations Verifications Reconciliations Performance reviews Systems and asset security Segregation of duties
Information and communication	To ensure individuals have information necessary to perform their responsibilities	Collecting information Analyzing information Communicating information Reporting information
Monitoring	To ensure the quality of internal controls over time	Ongoing monitoring of systems performance Supervision of employee activities Monitoring of control compliance Periodic effectiveness evaluations

Source: (Adapted from COSO, 1992).

ERP Systems

ERP systems play a critical role in implementing effective internal controls and business best practices in firms. ERP systems are comprehensive packaged software applications that automate and integrate organizational business processes across functional areas. Recognized as one of the most significant and widely adopted innovations in management information systems (Al-Mashari, 2002), ERP systems mark a major shift from proprietary made-to-order or homegrown legacy systems to generic off-the-shelf and vendor-developed applications (Davenport, 2000). ERP systems provide organizations with an environment for process remodeling and introducing best practices. Organizations, however, cannot just depend only on advanced information technologies to produce competitive advantage and business benefits (Powell and Dent-Micallef, 1997). The implementation of information technology to support business processes in innovative ways, and the development of complementary business and human resources to exploit the new capabilities, are critical for deriving sustainable long-term business benefits from ERP systems.

Furthermore, ERP systems, which are the primary means of compliance for most firms, as well as the regulations themselves, are dynamic and continuously evolving (Bititci *et al.*, 2000). For example, new technological developments and organizational learning can provide needs and opportunities for redesign and continuous development of ERP systems. New knowledge and organizational learning can provide ways for organizations to respond to uncertainties in the global environment (Harrison and Leitch, 2000). In addition, regulatory requirements can vary in different environments and evolve in multiple stages as experience grows (Bratton, 2003), and also require further systems modifications. Such dynamic environments can require innovative approaches and continuous monitoring, evaluation, and complex adjustments to controls, processes, and systems.

Complying with SOX regulations requires significant reconfiguration and additional design, evaluation, and reporting features in the ERP systems of most organizations. As such, they have substantial implications for both functional and technical features of ERP systems. Functional features, which are often driven by the performance management information needs of the organization, can effectively record accounting transactions, track key performance measures for evaluating internal controls, report them to individuals responsible, flag any violations for investigation, and provide a platform for benchmarking such information, for example, using balanced scorecards (Kaplan and Norton, 1996). ERP systems thus enable organizations to provide more frequent, timely, and integrated financial and non-financial reports to management, regulators, and auditors on control compliance (Matolcsy *et al.*, 2005). The key technical features of ERP systems, which heavily rely on advanced information technology (IT), include scalable client server software architecture, supported by a common relational database and a single development environment. Such features are capable of facilitating real-time integrated processing and management of information across all functional areas, as well as supply chain and customer relationships management (Kumar *et al.*, 2003; Davenport, 2000). The understanding of business processes and policies, and how business processes are related to one another, is important for achieving integration (Kumar *et al.*, 2002).

The role of IT in SOX compliance is particularly critical in large global organizations. For example, such organizations need a centralized and collaborative system to document their internal controls, processes, and control environment. Documentation on the development, implementation, maintenance, and effectiveness of internal controls should be accessible anytime to relevant employees and process owners across the organization through a secure and auditable system. Advanced IT solutions can help them collaboratively create and manage digital documentation, allowing world-wide access via corporate

intranets with a single authentication and access security system. Similarly, monitoring the control environment requires IT features capable of verifying and evaluating systemic controls within the financial systems, flagging control violations, and documenting remedial actions. These objectives can be achieved by building internal control and data integrity check points in the financial modules of ERP systems, or by integrating an external monitoring system with specific event-based controls within the financial modules.

In the IT-driven ERP systems, ensuring effective controls over the IT environment is critical for implementing SOX compliance. The IT Governance Institute (ITGI) (2004, 2006) has developed a framework for evaluating controls over IT processes, called Control Objectives for Information Technology (COBIT), which, among other things, specifically addresses the internal control needs of SOX. The framework provides 34 control objectives grouped into four main domains: plan and organize, acquire and implement, deliver and support, and monitor and evaluate; and maps them against the five COSO (1992) control areas. The framework thus helps align the internal control requirements of SOX and the IT systems features necessary for implementing them.

Implementation Challenges

Several challenges can exist for organizations in implementing internal controls and processes for SOX compliance. ERP systems must be capable of accommodating various conditions and information requirements in different countries and environments. For example, Brown and Nasuti (2005) reported that CIOs have cited problems with data structures, difficulties in ensuring adequate security and business continuity, and variations in infrastructure between business units as the top four obstacles to SOX implementation. In particular, outsourcing programming and network security can impact SOX compliance and need to be carefully managed. Nonetheless, the Deloitte & Touche (1999) survey indicated that "people problems" account for almost two-thirds of obstacles to successful ERP implementation (cited in Brown and Nasuti, 2005). Sohal *et al.* (2001) found that economic factors, lack of top management support, and difficulty in justifying costs were main impediments to IT implementation. However, there is some evidence that the most recent ERP applications are better able to accommodate some of these demands. For example, Robinson (2000) noted that the latest ERP systems are designed to address some global needs, for example, to comply with both international and US reporting standards, and to provide real-time financial information to global investors who are beginning to demand it.

Additional challenges can also stem from organizational structure and culture. For example, Mills *et al.* (1995) identified organizational culture as one of the key organizational constraints in implementing manufacturing strategy and processes. Beliefs, values, and expectations embedded in organizational culture evolve slowly and are difficult to change quickly, resulting in reluctance to change. Kennerley and Neely (2002) identified the most important barriers to facilitating systems evolution to be the lack of effective processes, necessary skills, and human resources; inflexibility of ERP systems; and inappropriate culture. These barriers were manifest in ad hoc systems, resistance to change, and the lack of appropriate measures and rewards. Bourne *et al.* (2002) examined both drivers and barriers of successful implementations. The two most important drivers of success were top management support and ultimate benefits that exceed costs. The four most important barriers, which successful implementers were able to overcome, were: difficulties with data access and information technology; time and effort required to set up systems, collect data, analyze data, and report results; difficulties concerned with developing appropriate measures; and personal consequences, for example, reluctance to implement measures and to report problems. Such

challenges can be further amplified, if the companies operate in several countries, subject to geographic, linguistic, and regulatory environments.

3. Methodology

The objective of this study is to enhance the understanding of challenges firms face in enhancing their ERP systems and business processes for SOX compliance. The study is exploratory in nature, since not much past research is available. Case study methodology has been adopted because it is extremely valuable in exploring and understanding phenomenon in the context and settings of organizations. Despite being criticized for being less rigorous, the case study has been used widely as a research methodology for observing and exploring complex phenomenon (Yin, 2003). Road maps for case study research provided by Eisenhardt (1989), Yin (2003), and Miles and Huberman (1994) can be used to ensure validity of the research.

Data were collected through case studies of four multi-site ERP-adopting organizations and secondary sources, such as magazine and journal articles, and websites. Focus group or individual interviews were conducted with senior systems managers/directors of the four organizations. One organization is listed on both the New York Stock Exchange (NYSE) and the Toronto Stock Exchange (TSX), one on both the NYSE and the Euronext, and two on the TSX. These organizations are thus required to comply with SOX requirements and/or similar Canadian internal control regulations. The effective compliance dates for the implementation of internal control systems in all four organizations are for fiscal years ending in 2006 (after July 14, 2006 for SOX and after June 29, 2006 for Canadian regulations). As such, all four organizations must have already implemented significant controls at the time of this study in order for them to comply with these deadlines. However, none of the organizations were required to have implemented auditor certification requirements, which are subject to extended deadlines (fiscal years ending after July 14, 2007 for SOX and yet to be announced for Canadian regulations). All four organizations use ERP solutions provided by major vendors (SAP and Oracle), which were in place prior to beginning the implementation of the regulatory internal control requirements. For confidentiality reasons, the organizations cannot be identified; however, but a brief profile of the four organizations, labeled Organizations A, B, C, and D, is provided in Table 2.

Table 2

Profile of Sample Organizations

	Organization A	Organization B	Organization C	Organization D
Operations	Canada and US with some marketing in Europe and Asia	More than 130 countries	Canada and US	Canada, US, Europe and Asia
Industry	Forest Products	Communications	Professional Services	Telecommunication
No. of Employees	More than 10,000	More than 58,000	More than 2,200	More than 750
ERP Software	Oracle	SAP and Oracle	SAP	SAP
Approximate Sales (USD)	More than 3 billion	More than 10 billion	More than 150 million	More than 150 million

4. Results and Discussion

Technical features of ERP systems play central roles in implementing SOX and internal control compliance in all four organizations studied. The participants identified three categories of technical features as particularly important: systems flexibility, systems security, and control adequacy. All four organizations used a systematic implementation approach, but needed to establish significant monitoring and auditing mechanisms. In three organizations, the necessary enhancements to the ERP systems were accomplished as part of broader change management and quality management initiatives. Throughout the implementations, all organizations had to overcome various cultural challenges. Each of these issues is discussed in this section, and the main implementation challenges are summarized in Table 3.

Systems Flexibility

All four organizations use one of the two major ERP applications (SAP and Oracle), but some modifications were needed to the standard modules to implement some SOX control requirements. For some control requirements, solutions outside the ERP systems were also needed. In some cases, ERP systems were found to be somewhat inflexible, allowing only certain types of modifications. In other cases, the required ERP systems modifications would have been too costly. Some differences in the adaptability and flexibility between SAP and Oracle were also noted. One respondent indicated that once a commitment is made to a certain application, "we are stuck", as it is too complicated and expensive to change to other systems. Another respondent expressed the limitations of ERP systems as follows:

> There are several things we can do within the system, which we are doing outside the system now. However, doing them within the system is not easy and straight forward; you cannot achieve it without a lot of customization and programming and workarounds.

Differences between the ERP applications were also noted, as expressed by one respondent:

> The main issue with [name of application] is … that there was a lot more control put in the user's hands in terms of not just access but also change management …[It] allows more 'open windows' in the access than [name of another application].

In other cases, changes to the ERP systems would have been too costly to warrant their implementation. In these cases, external add-on applications were used, as demonstrated by the following comment by one respondent:

> In some of the requests … it would have been cost prohibiting for us to make that change right and the benefits of making it didn't outweigh the costs, or the costs outweighed the benefits, so [we had to] get an [outside] solution … to comply with that control objective…

A reasonable degree of systems flexibility is desirable in effective systems to reduce excessive 'red tape', but it has to be carefully balanced with loss of systems security and control, i.e., an effective balance needs to be struck between flexibility and control.

Systems Security

Systems security was a particularly important technical issue in all organizations. Systems security can involve data security, for example, password protected data access; asset security, for example, segregation of duties and inventory control procedures; and physical plant security, for example, electronic surveillance and restricted entry to buildings. A particular concern for improving systems security was the existence of "bolt-on" systems, which are locally managed applications, not part of the centrally administered ERP systems. Different individuals could make changes to the systems, causing problems for establishing process responsibilities and data security. In one large global organization, "bolt-on" systems posed particular problems, as different ERP applications were used in the operations of some countries. The organization ultimately changed to one application for its SOX implementation in all operations, for the following reasons expressed by the respondent:

> There were a lot of bolt-on systems that were also outside the management of your typical IT/IS area… We were really surprised to see how much change management….an end user within a functional area outside of IT could do to a system … that we had in [name of country].

In another organization, the respondent expressed a similar frustration as follows:

> …[I]t was vulnerability of the bolt-on systems into our ERP system. So we changed the access password and we have a compliance of x number of characters, and change had to occur 90 days after the first…What happened was that a couple of business communities had bolt-on systems that were serviced outside the IS/IT system that had feeds into our ERP system that we didn't know about.

Table 3

ERP Systems Challenges in Implementing SOX Compliance

Challenge/Weakness	Examples
System Flexibility	• ERP applications (SAP, Oracle) required some modifications for SOX • Some ERP systems modifications possible, but too costly • Some differences in flexibility between ERP applications (SAP, Oracle) • For some SOX controls, technical solutions outside ERP needed • Balance between systems flexibility and adequate controls
Systems Security	• Process ownership and accountability sometimes difficult to implement • Data security sometimes compromised and needed to be enhanced • Local "bolt-on" systems problematic for establishing systems-wide controls
Control Adequacy	• Many controls already in place, but needed to be formalized and documented • Additional data input and output controls needed • Segregation of duties key control mechanism • Segregation of duties more difficult in smaller organizations
Implementation Processes	• SOX implementations, on average, 80-95 percent complete as to IT • Progress slow in some cases and more time needed than expected • Thorough business process analysis needed first • External consultants and/or auditors engaged by all companies • Ambiguity about control requirements, particularly in early stages • Shifting compliance timelines for some requirements • Lack of resources and vendor support, particularly for smaller organizations • SOX compliance as part of broader strategic change management initiatives
Monitoring Processes	• Identifying users and their information needs • Monitoring data use patterns • Restricting access on need-to-know basis • Controlling remote access • Adjusting processes and controls based on monitoring
Auditing Processes	• Providing reliable process documentation • Providing transparent audit trail for tracking processes and transactions • Evaluating and reporting control effectiveness • Balancing control tightness, costs, and benefits • Promoting accountability for processes and results
Cultural challenges	• Resistance to change • More limited systems access problematic to existing users • Resistance to decreased individual controls and increased centralized controls • Lack of understanding of other cultures • Different standards, rules, and terminology in different countries

Control Adequacy

The respondents from two of the four organizations indicated that adequate systems controls were already in place before beginning SOX implementation, and the major task was "formalizing" the controls systems and documenting the controls and related processes. A respondent from one of these organizations reflected on control adequacy as follows:

> A lot of it [control implementation] is formalizing what you already do, at least that is what we found especially in my group because a couple of people who worked for me were consultants, so they are used to documenting…So we always said that we believe what we are doing is right and now it is a matter of documenting it and getting approval…

On the other hand, significant new controls were needed in the other two organizations. In one organization, approximately sixty new control processes were needed, many related to inventory management. In the other, systems security and segregation of duties required attention. The respondent from this organization commented on a need for additional controls as follows:

> We had a number of things that were implemented mostly around security. An easy way to identify segregation of duty activities was key, also 'sniffing' and monitoring of our systems and more stringent controls around where the data is going and what is coming into our systems, and how they are being accessed in terms of password control and [making] changes…

Segregation of related duties in processing financial transactions is one of the key control requirements of SOX. Its purpose is to assign related tasks, for example, handling cash deposits and recording cash transactions, or handling cash receipts and cash payments, to different individuals, in order to prevent one individual from stealing cash and falsifying the records to cover up. Generally, segregation of duties by making changes to ERP systems was relatively more difficult for Organizations A, C, and D than for Organization B, which can afford its own ERP competency center given its larger size. In addition, in smaller organizations, the finance function may not be large enough to warrant several finance clerks, which may be necessary to properly segregate their duties in accordance with SOX. However, Organization B also provided examples of difficulties in segregating duties in its smaller operations, as expressed by the respondent:

> So we have different divisions on our ERP system. We had smaller type units where they said [name of company] …[must] segregate an Accounts Payable clerk from an Accounts Receivable clerk, but we have one clerk and they're AP/AR and we need both accesses…It was a matter of then going through which [has] the higher potential risk.

Implementation Processes

All sample organizations used a systematic approach to implementing SOX and internal control compliance. The respondents for the two larger organizations expressed a high degree of completion of SOX requirements, in the 80-95 percent range for systems and IT, but also recognized that some functional areas still have significant work to do. However, it is notable that one organization suspended its registration with the NYSE for one year, reportedly to "buy another year" to comply with SOX. The degree of completion for the two smaller organizations is somewhat lower, approximately 70 percent, which is understandable given the extended compliance dates for smaller organizations and for non-US organizations.

In all four organizations, SOX and internal control implementations required the identification, analysis, and evaluation of business processes and assigning process responsibilities and process ownership. All organizations involved auditors in these processes, and larger organizations also used consultants to analyze and document processes and to design appropriate controls. In three of the four organizations SOX implementation was part of a broader "quality management" or "change management" implementation initiative. For evaluating IT controls, all organizations used the COBIT framework of the IT Governance Institute (2004, 2006). While all organizations were not clear at the beginning of SOX implementation what the specific requirements were, the larger organizations appear to have been able to formalize the existing controls and processes, and to implement the necessary new processes and controls, with help from auditors and consultants. However, the smaller organizations still appear to be struggling with some aspects of implementation. The respondent from one of the smaller organizations expressed their difficulties as follows:

> We found that even for [name of auditing firm] it was difficult because the rules were still changing… You are trying to get it implemented because there are [sec] deadlines, but the authorities still haven't totally defined what they are looking for.

> The key to the change management system is that you have to make it scalable to your business. Obviously we are small; we couldn't have a big fancy system. So…we continue to use our help desk package …[to] track it, and we designed some [simple] forms …and we get that approval [for these process]…the key issue with any change within the system is getting somebody outside the group to take responsibility for that change.

SOX implementation is costly and time-consuming for all organizations. All four organizations indicated using services of major auditing firms at least in the initial stages of their compliance projects. The high compliance costs have also resulted in some organizations questioning: Have we gone too far with control legislations? Are there benefits of doing this? One of the organizations is apparently spending approximately three percent of its revenues on compliance projects. The respondent from this organization commented on the processes and costs as follows:

> It [has] been four years now; we are constantly going through control and process clean-up….It is the same people [management, auditors, and consultants] redefining it, redefining it, and … the internal auditors aren't even clear what has to happen. But one thing is that they are sure that their budget for the entire interim control process for [name of organization] …is just going up and up. Right now, if I remember it right, it is almost 3-4% of our revenue, which is really, really high.

The financial implications of SOX implementation in smaller organizations are intensified by the lack of adequate support from systems vendors. Although all organizations, except for Organization A, use an ERP application from the same vendor, the smaller organizations found it more difficult to get information and support from the vendor. Smaller organizations were also not able to participate actively in user groups and forums through which vendors provide new information to customers.

Monitoring Processes

An important component of SOX compliance is the establishment of ongoing systems monitoring and evaluation to ensure continuous compliance after the initial controls and processes have been established. Based on monitoring feedback, the controls or the related processes may need to be adjusted. Some areas of monitoring include: where the data is going, how and by whom it is being accessed, and security of other applications and interfaces. For example, in one organization, managers need to sign off on who needs systems access, systems use patterns are continuously monitored, and systems access withdrawn for non-use. However, the respondent from this organization encountered an implementation problem as follows:

> [We have been] putting a lot of these 'sniffing things' on the servers, host intrusion protection systems and stuff like that [and] also had…managers sign off on people who had VPN remote access…[but when] I gave all …business process owners [list of] the users and all the roles they have, I would get it back within an hour, so I really question how much they really are looking at it.

As another example of need for improved systems monitoring, in one large global organization a new user account was often created by making a copy of an old account rather than making a new account to reflect the roles and responsibilities of a new employee or position. For SOX compliance, ERP systems had to be updated to ensure that users were no longer able to access information that was not necessary for them to carry out their job responsibilities. The following comments by the respondent from this organization demonstrate this problem and a solution to it:

> …[If] a new user comes on board, sometimes what they try to do is copy someone's account. So I am a new account AP clerk, give me the same [access] as Joanne… but Joanne used to work in manufacturing. Did we strip her of her production control transactions that would conflict with the [responsibilities of] AP clerk?

> We actually created a new type of report on [name of ERP application]…at the database level as well as the transactional level, and we identified key transactions within the ERP system that would line up against typical user account. So [for] an AP clerk or an ITBSA, you know what transactions would they hit, and which transactions would conflict… It is a [huge] report…like a tree mapping, so we can identify how many non-compliance issues we have with user access.

Auditing Processes

The documentation of internal controls and processes that is required by SOX creates an audit trail, enabling the processes to be reliably repeated and any deviations from standard processes investigated and adjusted, if necessary. A transparent audit trail promotes the visibility of and the accountability for processes and operating results. It is also necessary for granting a "clean audit opinion" on the effectiveness of internal controls and processes by external auditors. It is particularly important in large global organizations with diverse operations and environments. When establishing auditing and investigation procedures, it is important to consider the relative importance or materiality of each control or process in

order to ensure that the benefits from investigations exceed the related costs. There is a need to strike a delicate balance between improved control and efficiency on one hand, and the risk of material errors, omissions, and misstatements in input data and output reports on the other. The respondents expressed the importance of these notions as follows:

> If someone goes in and updates the number, we know through the authorization who is capable of doing it, and it might be easy to identify through an audit trail.

> Different systems have different [materiality criteria], depending on how you configure it [sic]…Different limits could be by dollar value [or] by percent of invoice value…It was a matter of getting the process owner to define the rule.

> They and we [regional teams for different countries] have one system that we put all our controls on, so it is visible world-wide, so the other countries can see how we are doing, and how we are doing against it [sic]… From a global perspective there is a lot of co-sharing. You know processes and challenges and so forth, similarly so [does] our global group audit service…

Cultural Challenges

A major cultural factor affecting SOX implementation in the four organizations was resistance to change. The loss of data access and authority seemed to cause significant problems to users. With restructured and streamlined processes, some jobs and responsibilities changed and security procedures increased. Some users did not like the increased restrictions placed on their work activities and data access, and did not understand or appreciate the value of new processes and procedures. The resistance was more prominent on the part of users in other countries, as they perceived SOX implementation as a centralized control activity, not necessarily affecting or benefiting them. One respondent described the loss of data access resulting in:

> … an insecure feeling that maybe that person is not important anymore in the company, [as] you are taking away some of the authorization [and] you are segregating the duties, so they couldn't accept that.

Another important cultural factor was differences in rules and business conduct in different countries. Different countries have different accounting rules and different approaches to controls. For example, some countries follow their own national accounting standards, which can vary from country to country, whereas some others have adopted international accounting standards. Different accounting rules may require different information or similar information reported in different ways. In addition, at least one large Asian country has strict rules on what information can be reported and accessed on the internet, whereas other countries require reporting of corporate financial information in public on-line data bases. One respondent expressed a concern about the reliability of financial information as follows:

> I would say that the biggest challenge is where there are global applications serving multiple different countries…by their financial reporting system that everybody feeds into.

> Unless you have all the terminology all the same, it is not going to necessarily line up similarly with sharing of data, and the ability to change data…

In order to facilitate global co-ordination throughout its control implementation process, one large organization established a cross-functional global team to ensure the visibility and co-sharing of local and global changes to business processes. This organization needs to comply with several local and global requirements throughout its operations in several countries. The collaborative process required the creation of shared terminology and reporting rules. In order to manage these processes, the organization developed a tool, which involved defining top level control objectives, sub-objectives, and steps within sub-objectives. The respondent from this organization expressed the basic structure of this initiative as follows:

> We have structured ourselves for Sarbanes-Oxley, we have regional teams that are kind of compliance groups. Then within each of the regional teams, you have representatives from IT, finance, and operations… Then at the global level, we have a global representative that is from GAS or group audit services, which is an internal auditing team, as well as security.

In other cases, compliance with regulations of foreign country can also affect the culture of the host country, by forcing local organizations to adopt different processes and ways of doing business, and vice versa. The following examples given by the respondents demonstrate this point:

> European partners have a different interpretation of user acceptance testing; how much we should share with clients and what level of access should we provide to customers. Our overseas partners had different opinions on such issues. In US, all kinds of regulations exist around technology, while EU partners have different level of technology sharing.

> How our partners manage and record hours spent on R&D is different the way we do. In UK, for example, they tend to audit more diligently and detailed on skill level, on approval processes related to inventory management, and how outsourcing decisions are taken.

> Initially the corporate office here had a hard time accepting the rules what were proposed by all the project managers in Europe, saying no this is not how we want the accounting because we follow totally different rules.

5. Conclusion

This study examines the challenges faced by large and medium-sized public companies in enhancing their ERP systems for SOX compliance. The results provide an overview of some technical, process, and cultural challenges, which can serve as guidance to operations and systems managers in en-

hancing their operational processes and ERP systems, as well as a foundation to researchers in building a model of ERP systems effectiveness in implementing effective controls.

ERP systems provided a technological platform in all organizations for successful SOX implementation, but they were not able to meet all control requirements without significant modifications, or in some cases, additional add-on applications. All four organizations use one of the two major ERP applications (SAP and Oracle), but some modifications were needed to the standard modules to implement some SOX control requirements. Some solutions outside the ERP systems were needed due the inflexibility of ERP systems or high cost association with modifying ERP systems. As to functional uses, the respondents provided examples of using ERP systems for meeting various information needs, such as planning, monitoring, controlling, evaluating, reporting, inventory management, supply chain management, and change management.

SOX implementation in all organizations has been a long, complicated, and costly process, which is not yet fully complete. The main challenges initially facing all organizations were resistance to change and the lack of proper implementation guidance. Audits firms and consultants were generally engaged early in this process. In all cases, detailed analyses and documentation of existing systems, controls, and processes were completed. On the technical side, systems security and segregation of duties were seen as major challenges. These challenged were often associated with "bolt-on" systems, which were locally managed applications, not part of the centrally administered ERP systems. Some organizations also approached the SOX implementation as part of a major business improvement project, for example, change management or quality management program. It is evident that all organizations have been spending a great deal of effort and resources on their compliance projects.

Different systems, cultures, and rules posed some additional obstacles. For example, in one organization, two different ERP applications were used in different countries, complicating the standardization and documentation of some processes required by SOX. Resistance to change, although encountered in all operations, was more prominent on the part of users in global operations, as SOX implementation was perceived as a centralized control activity, not necessarily affecting or benefiting them. Furthermore, different countries have different accounting rules and different approaches to controls, complicating the implementation of controls and consistency of financial reporting. Nevertheless, most organizations have been able to address such challenges quite successfully and regard their own progress to date at least as satisfactory.

6. References

Al-Mashari, M., "Enterprise Resource Planning (ERP) Systems: A Research Agenda," *Industrial Management & Data Systems*, 102 (3), (2002), 165-170.

Bititci, U. S., Turner, T., and Begemann, C., "Dynamics of Performance Measurement Systems," *International Journal of Operations &Production Management*, 20 (6), (2000), 692-704.

Bourne, M., Neely, A., Platts, K., and Mills, J., "The Success and Failure of Performance Measurement Initiatives: Perceptions of Participating Managers," *International Journal of Operations &Production Management*, 22 (11), (2002), 1288-1310.

Bratton, W. W., "Enron, Sarbanes-Oxley and Accounting: Rules versus Principles Versus Rents," *Villanova Law Review*, 48 (4), (2003), 1023.

Brown, W., and Nasuti, F., "What ERP Systems Can Tell About Sarbanes-Oxley," *Information Management & Computer Security*, 13 (4), (2005), 311-327.

Canadian Securities Administrators, "CSA Staff Notice 52-316: Certification of Design of Internal Control Over Financial Reporting," (2006), http://www.osc.gov.on.ca/Regulation/Rulemaking/Current/Part5/csa_20060922_52-316_certification-design.jsp [Accessed 29 October 29 2006].

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management: Integrated Framework (Executive Summary)*, (2006), http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf [Accessed 28 October 2006].

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control: Integrated Framework (Executive Summary)*, (1992), http://www.coso.org/publications/executive_summary_integrated_framework.htm [Accessed 2 April 2006].

Davenport, T. H., *Mission critical: Realizing the Promise of Enterprise Systems*, Boston, MA: Harvard Business School Press, 2000.

Eisendhart, K. M.,"Building Theories from Case Study Research," *Academy of Management Review,* 4 (4)**,** (1989), 532-550.

European Parliament and Council, Directive 2006/46/EC, (2006), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0046:EN:NOT [Accessed 28 October 2006].

Harrison, R. T., and Leitch, C. M., "Learning and Organization in the Knowledge-Based Information Economy: Initial Findings from a Participatory Action Research Case Study," *British Journal of Management*, 11, (2000), 103-119.

IT Governance Institute (ITGI), *IT Control Objectives for Sarbanes-Oxley: The Importance of IT in the Design, Implementation and Sustainability of Internal Control over Disclosure and Financial Reporting*, (2004), http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=24235 [Accessed 17 October 2006].

IT Governance Institute (ITGI), *COBIT Mapping: Overview of International Guidance*, 2nd Edition, (2006), http://www.itgi.org/AMTemplate.cfm?Section=Deliverables&Template=/ContentManagement/ContentDisplay.cfm&ContentID=24759 [Accessed 17 October 2006].

Kaplan, R. S., and Norton, D. P., *The Balanced Scorecard: Translating Strategy into Action*, MA: Harvard Business School Press, Boston, 1996.

Kendal, K., "A ten step Sarbanes Oxley solution," *Internal Auditor*, (December 2004), 51-55.

Kennerley, M., and Neely, A., "A Framework of Factors Affecting the Evolution of Performance Measurement Systems," *International Journal of Operations &Production Management*, 22 (11), (2002), 1222-1245.

Kumar, V., Maheshwari, B., and Kumar, U., "ERP Systems Implementation: Best Practices in Canadian Government Organizations," *Government Information Quarterly*, 19 (2), (2002), 145-172.

Kumar, V., Maheshwari, B., and Kumar, U., "An Investigation of Critical Management Issues in ERP Implementation: Empirical Evidence from Canadian Organizations," *Technovation*, 23 (9), (2003), 793-807.

Markus, M. Lynne, and Tanis, Cornelis, "The Enterprise System Experience: From Adoption to Success," in *Framing the Domains of IT Management: Projecting the Future through the Past*, Zmud R. W. (ed.), Pineflex Educational Resources Inc., 2000.

Matolcsy, Z. P., Booth, P., and Wieder, B., "Economic Benefits of Enterprise Resource Planning Systems: Some Empirical Evidence," *Accounting and Finance*, 45, (2005), 439–456.

Miles, M. B., and Huberman, A. M., *Qualitative Data Analysis: An Expanded Sourcebook*, Thousand Oaks CA: Sage Publications, 1994.

Mills, J., Platts, K., and Gregory, M., "A Framework for Design of Manufacturing Strategy Processes: A Contingency Approach," *International Journal of Operations &Production Management*, 15 (4), (1995), 17-49.

Powell, T. C., and Dent-Micallef, A., "Information Technology as Competitive Advantage: The Role of Human, Business and Technology Resources," *Strategic Management Journal*, 18 (5), (1997), 375-405.

Robinson, T. R., "The Global e-Economy: Can Your ERP Handle It?", *The Journal of Corporate Accounting & Finance* (September/October), (2000), 15-18.

Sohal, A. S., Moss, S., and Ng, L., "Comparing IT Success in Manufacturing and Service Industries," *International Journal of Operations &Production Management*, 21 (1/2), (2001), 30-45.

Yin, R. K., *Case Study Research: Design and Methods* (3rd Ed.), Beverly Hills CA: Sage Publications, 2003.