

## ACHIEVING SARBANES-OXLEY COMPLIANCE WITH XBRL-BASED ERP AND CONTINUOUS AUDITING

Yuan Li, The University Of Texas Pan American, [yli1@panam.edu](mailto:yli1@panam.edu)  
Joseph N. Roge', The University Of Texas Pan American, [jroge@panam.edu](mailto:jroge@panam.edu)  
Les Rydl, The University Of Texas Pan American, [lrydl@panam.edu](mailto:lrydl@panam.edu)  
Jerald Hughes, The University Of Texas Pan American, [jhughes1@utpa.edu](mailto:jhughes1@utpa.edu)

---

### ABSTRACT

*The Sarbanes-Oxley Act (SOX) of 2002 places significant and costly new burdens on public companies. Meeting the recurring requirements for financial reporting under SOX effectively will demand innovative application of information technology. The Continuous Auditing Web Services model (CAWS) provides a framework for considering how to efficiently manage and automate financial reporting. We propose extending the basic ideas behind CAWS, to leverage the flexibility and power of Extensible Business Resource Language (XBRL) in Enterprise Resource Planning (ERP) systems. The resulting comprehensive IT support for financial reporting, auditing, internal control, and monitoring functions will enable corporations to achieve SOX compliance in a timely, sustainable and cost-effective manner. Our analysis demonstrates the appropriateness of the XBRL-based solution by showing how the capabilities of such a system can address the specific requirements imposed by SOX.*

**Keywords:** Information Technology (IT), Ethics, IT and Ethics

### INTRODUCTION

In 2002, a number of major corporate and accounting scandals involving prominent companies in the U.S. motivated Congress to enact the Sarbanes-Oxley Act (5), in order to assure investor confidence in the integrity of the capital markets. The Act has the following significant effects on public companies. First, it speeds up financial reporting by requiring public companies to file quarterly reports within 35 days of the close of the quarter and annual reports within 60 days of the close of the year. Disclosures of "material events" and insider trades must be filed within 2 days of the events. Second, section 302 of the Act mandates that chief executive officers (CEO) and chief financial officers (CFO) must sign on to the financial reports, and must certify that they are "responsible for establishing and maintaining internal controls", and that they "have designed such internal controls to ensure that material information relating

to the company and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared." The officers must "have evaluated the effectiveness of the company's internal controls as of a date within 90 days prior to the report" and "have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date." Third and finally, section 404 requires management to produce an "internal control report" as part of each annual Exchange Act report. The report must affirm "the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting." The report must also "contain an assessment, as of the end of the most recent fiscal year of the Company, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting."

A top concern raised by SOX is the cost of implementing the new requirements of section 404. Both smaller and larger public companies have identified the internal control provisions in section 404 as the most costly to implement. According to a report submitted to the Congress by the U.S. Government Accountability Office, for companies with market capitalization over \$700 million the median audit fee to comply with SOX was 0.25% of revenue; for companies with market capitalization below \$75 million the fee was 1.14% of the revenue [21]. Out of concern for the impact of SOX compliance requirements, the Security and Exchange Commission extended the section 404 deadline for smaller companies with less than \$75 million in market capitalizations to 2007.

The need to address the mandates of SOX presents public companies with a problem of information collection and processing. To comply with the Act, company CEOs and CFOs need to be able to audit and verify each step in a transaction, from order, to payment, to storage of data, and to aggregation into financial reports. Information Technology (IT) is thus critical for achieving compliance cost-effectively.

Systems such as ERP are required to be deeply integrated into the creation, authorization, and reporting of financial data. The systems' document management, access to financial data, and long-term storage of information must provide auditing capabilities.

Because the Sarbanes-Oxley Act has demanded complicated and time-consuming processes from public companies and placed legal liability for financial reports on management, public companies are being pushed to find a cost-efficient way to comply with the Act. Our study focuses on sustainable compliance with SOX, which includes financial information and the internal controls audit. In this study, our goal is to explore how XBRL-based ERP systems for continuous auditing can enable public companies to keep sustainable compliance with SOX. The remainder of the paper is organized as follows: Section 1 will briefly explain the auditing and control requirements of SOX; Section 2 will introduce the notion of *continuous auditing* as it applies to the SOX problem; Section 3, our primary contribution, will explain the advantages of XBRL-based ERP systems for SOX compliance; Section 4 will conclude with some challenges and issues associated with our proposed solution.

### AUDITING AND REPORTING REQUIREMENTS FOR SOX

Auditing exists because of the separation of ownership and control [15]. "Auditing is the accumulation and evaluation of evidence about information to determine and report on the degree of correspondence between the information and established criteria. Auditing should be done by a competent, independent person [2]." According to this definition, there are five elements in auditing: 1). Information in a verifiable form; 2). Established criteria by which the auditor can evaluate the information; 3). Evidence; 4). Independent auditor; 5). Report. Typically there are three types of audits: operational audit, compliance audit, and financial statement audit. The auditing evidence includes physical examinations, confirmation, documentation, analytical procedures, inquires of the client, reperformance, and observations [2]. Before SOX, the public certified accountant (CPA) firms focused only on financial statement audits for companies filing reports to SEC. SOX adds a report for companies about their internal control related to its financial reporting and requires CPA firms to attest it as well.

A system of *internal control* consists of policies and procedures designed to provide management with reasonable assurance that the company achieves its objectives and goals. Internal controls play a role in helping companies meet the financial reporting objectives [4].

Management typically has three broad objectives in designing an effective internal control system: reliability of financial reporting, efficiency and effectiveness of operations, and compliance with laws and regulations. SOX requires that management must evaluate the design of internal control over financial reporting and must test the operating effectiveness of those controls [2]. For the purposes of SOX compliance, the SEC has published the rules pertaining to the section 404 report and what it must contain. In addition to several statements of responsibility by both management and the auditors, these rules describe the specific internal controls which must be exercised:

"...policies and procedures that

- pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the registrant;
- provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and receipts and expenditures of the registrant are being made only in accordance with authorizations of management and directors of the registrant; and
- provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant's assets that could have a material effect on the financial statements." [20]

It is towards the performance of these required elements of SOX compliance that this discussion of information systems employing XBRL is directed.

### CONTINUOUS AUDITING FOR SUSTAINABLE COMPLIANCE WITH SOX

In response to a series of business scandals, the SEC and the AICPA have advocated greater reliance on continuous assurance, which utilizes on-line information technology to produce audit results. Automation of the monitoring financial process and the control activities enables a complete and accurate view of the control environment and a higher level of confidence [4]. In the past, several studies have

addressed the technical feasibility of continuous auditing of financial statements [10, 22, 23, 12, 24]. Elliott [9] reports that there is considerable demand for continuous auditing. Alles et al. [1] point out that the high costs of implementation may make continuous auditing difficult to adopt. However, while public companies are mandated to comply with SOX, continuous auditing is turning out to be a cost-saving process for repetitive reporting [17].

*Continuous auditing* has been defined by the CICA-AICPA<sup>1</sup> Joint Study Group [3] as “a methodology that enables independent auditors to provide written assurance on a subject matter using a series of auditors’ reports issued simultaneously with, or a short period after, the occurrence of events underlying the subject matter.” By this definition, continuous auditing for large public companies can only effectively be a technology-driven process in which control and risk assessments are performed automatically. As a result, instead of conducting periodic reviews of transaction samples, the company is engaged in the ongoing audit testing of all transactions [21]. This shift impacts the nature of the evidence as well as the timing, procedures, and levels of effort required by internal auditors.

Researchers have proposed some methods for facilitating continuous auditing. They focus on the use of embedded audit modules and their variants [10, 22, 3, 11]. Varsahelyi and Halper (1991) presented a continuous auditing implementation in a corporate setting. Murthy and Groomer proposed a continuous auditing web services (CAWS) model for XML-based accounting systems. These studies mainly focused on the financial statements audit. In the proposed CAWS model, “continuous auditing functionality is defined as a set of Web services that reside within the auditor’s computing environment rather than within the auditee’s computer system.” [14]

Continuous auditing has benefits for both the auditor and management. The continuous auditing process enables auditors to analyze data more frequently by performing control and risk assessments in a real-time environment. It provides an opportunity to go beyond the confines of traditional audit approaches, such as sampling and point-in-time assessments, to provide timely notification of control gaps and weaknesses, laying the groundwork for immediate follow-up and remediation. Continuous auditing also

improves an organization’s management and control frameworks by separating them from the underlying operational and financial systems. Integrated monitoring techniques can reduce error and fraud, increase operational efficiency and improve profitability by lowering costs and reducing overpayments and revenue leakage. They also facilitate the review of key business systems for anomalies at the transaction level and for data-driven indicators of control deficiencies and emerging risk, capabilities which directly address the internal controls required by SOX.

The responsibility for process documentation, testing, and any remediation or enhancement activities resides ultimately with management as required by SOX. Automation of these processes is essential to establishing a sustainable compliance framework. Automation of documentation, monitoring, testing, and enforcement can be made more stable and coherent through the application of information technology in managing compliance.

To continuously maintain compliance with SOX, the most cost-efficient approach for public companies is to implement an ERP system. Since compliance with the Act is a long-term program for companies, they cannot cost-effectively take a project-based approach to producing the required documentation and reports. The companies also cannot implement manual procedures or tactical workarounds based on internal control processes. The companies’ ERP system should integrate financial reporting and internal control functions to drive down costs and complexity in the most efficient way. Therefore, companies should take a strategic view of compliance by adopting a process-centric approach, with a focus on rationalizing their internal controls to ensure that the control framework is aligned with the key business drivers [4].

To summarize, IT-based continuous auditing functionality is a strategy for companies to reach sustainable compliance. Continuous online auditing reduces the time and costs of ongoing audits. Continuous auditing enables a shift from detective to preventive capabilities. The overarching goal is to achieve a state of pervasive compliance in which rationalized controls, embedded in optimized business processes, operate in real time to prevent compliance issues before they arise.

## **IT FOR CONTINUOUS AUDITING**

Information technology frameworks, such as extensible business reporting language (XBRL) and

---

<sup>1</sup>The Canadian Institute of Chartered Accountants and the American Institute of Certified Public Accountants.

Web services, can be utilized to facilitate continuous auditing. Relying on a number of components of Web services technology, Murthy and Groomer [14] presented the continuous auditing web service (CAWS) model for continuously auditing business processes. The primary user of CAWS is the audit firm itself. As seen in Figure 1 below, the CAWS model uses the emerging XML Web services framework to support a “pull model” of continuous auditing in a world of XML-enabled accounting systems. Murthy and Groomer also pointed out two paths that could be followed to realize a web-service-based approach to continuous auditing. One is to custom-develop an internal accounting system using Business Process Execution Language for Web Services<sup>2</sup> (BPEL4WS) as the underlying XML-based language. The second path involves the creation of XBRL General Ledger (GL) data hubs, which would serve as the intermediary between the internal accounting system of the target company and the auditor’s system, where the CAWS resides [14].

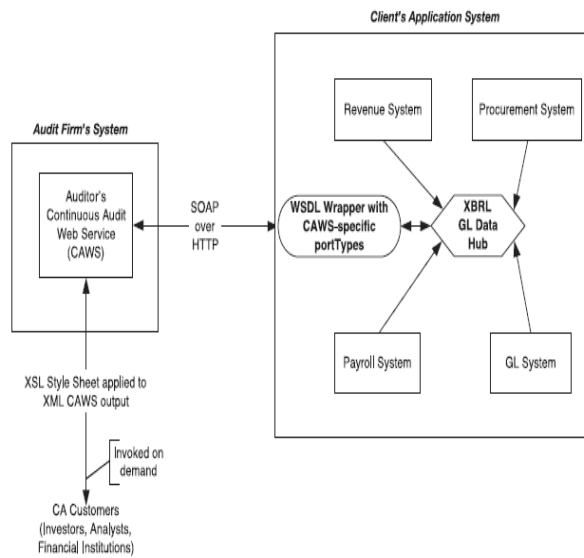


Figure 1: Murthy and Groomer’s CAWS model

**Proposed XBRL-Based ERP Model**

In Li et al 2006 [13], we addressed how XBRL can improve the transparency of financial information to creditors and investors. In XBRL, identifying tags are attached to items of data so they can be processed efficiently by computer software. XBRL is easily extensible and can be used across platforms, software formats, and/or technologies. These XBRL characteristics allow the complex, ever-changing

<sup>2</sup> BPEL4WS specification here: <http://www-128.ibm.com/developerworks/library/specification/ws-bpel/>

financial reporting process to become more efficient and economical. As a result, it is becoming increasingly popular in public financial reporting<sup>3</sup>.

We now propose to take the idea of a continuously auditing system from the CAWS model above, and extend it via the use of XBRL to address the mandates of SOX. The proposed ERP system with sustainable compliance to SOX can be built using XBRL technologies, incorporating both the XBRL general ledger taxonomy and the internal control taxonomy (see Figure 2 below). Using these tags, every data element is fully described in terms of its definition, format, location, calculation, and labeling. The tags themselves act like barcodes that stick to data regardless of their paths, destinations, or usages. XBRL can show how items are related to one another, and can also identify whether they fall into particular groupings for organizational or presentational purposes. When the auditor or management searches XBRL-formatted documents, all related information within the documents can be presented to them simultaneously. The XBRL taxonomy thus offers a powerful mechanism for XBRL-based organization systems to interface with one another. This XBRL-driven system provides opportunities for continuous auditing. In particular, using XBRL Web services technology, the continuous auditing mechanism can actually reside within the auditor’s system rather than the auditee’s systems, as in CAWS [14].

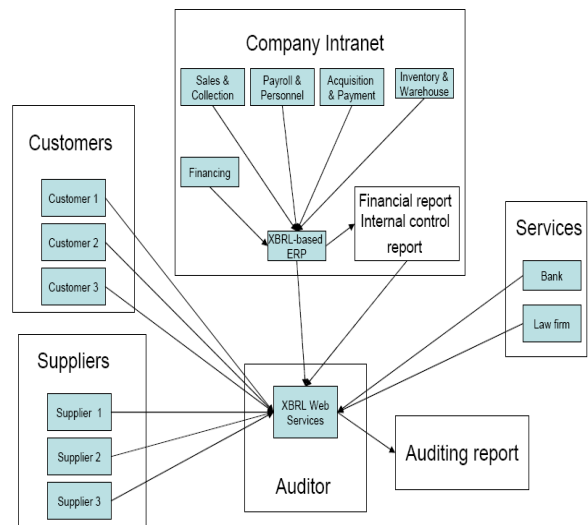


Figure 2: The proposed XBRL-based ERP system Real-Time Monitoring Tasks And Solutions

<sup>3</sup> See for example, <http://accounting.smartpros.com/x37643.xml>

In a database, integrity constraints are used as the principle tools to detect errors [7, 26, 16]. The integrity constraints are programmed controls integrated within a database management system (DBMS). The integrity constraints verify the objective behind each transaction and require that they are satisfied before an input is accepted for processing [7]. Monitoring a database at all times through the use of integrity constraints is the most secure approach to error detection because of its comprehensiveness. However, real-time monitoring in business operations could be extremely expensive if it resulted in significant delays in the transaction processing. Furthermore, the delay in the transaction processing could lead to additional errors because some of the data might be lost or become out-dated [18, 25]. These are some of the reasons why continuous monitoring is rarely used [17].

Transaction integrity monitoring systems continuously monitor 100 percent of the transactions and business activities in financial systems in real time to evaluate the compliance of every transaction and prevent losses associated with errors, misuses, and fraud. It can automate the analysis and testing steps in an audit, which reduces SOX monitoring and testing expenses. The real-time analysis prevents costly errors within procure-to-pay order-to-cash and financial accounting and reporting processes. In the proposed ERP model, instead of monitoring each transaction at the end point of the transaction process, we install the real-time monitoring reporting function behind the process. Therefore the transaction process goes smoothly without the interference of the monitoring process, but all abnormal results from the monitoring will be sent to an alert file to corresponding managers.

### **Automated Risk Assessment And Controls**

According to a special report of an electronic survey of 180 senior finance executives conducted by CFO Research Services in 2005, Sarbanes year-one efforts uncovered some key issues and enabled many companies to improve their compliance processes, mostly as a result of more thoroughly automating risk assessments and controls [4].

The proposed system can improve control environments by testing the segregation of duties. For example, the system can allow the creation of user profiles to closely track each user's job responsibilities. A report can be built into companies' enterprise systems, which then enables management to identify an employee whose functions are violating the segregation of duties; then the management can correct the conflict accordingly. Eventually,

companies can enhance their control environments and separate conflicting duties through ensuring that users' access and privileges within the company's information and decision-making chain are commensurate with their job responsibilities. That, of course, gives companies added protection against malfeasance. Therefore, the integration of this function could greatly reduce employee fraud. Automation of the testing of access controls and other types of testing makes the ongoing process less burdensome. This could be especially useful when it comes to tracking who has access rights to certain types of account information. System administrators are "superusers," able to assign access rights temporarily to other individuals. Automated testing means that the management has historical information of the whole period of time. The result is a timely and efficient means of ensuring segregation of duties.

A SOX compliance enterprise system provides more internal control resources and automates testing. Management is able to standardize and centralize more of its global financial processes in a shorter amount of time. A newly installed ERP system could facilitate the migration of some manual detective controls to more efficient, automated preventive controls [4]. Integrated analysis functions within the system enable the management to identify trends that run counter to the management's expectations, and integrated financial analysis functions will indicate an alert on unusual ratios, warning the management about any unusual departures from the company's historic records or from the industry average. Therefore, the proposed ERP system can verifiably improve the company's overall control capabilities.

### **Reduction In Cost**

The proposed ERP model could reduce auditing fees, because of sustainable compliance and reduced auditing risks. Continuous monitoring of controls improves accuracy in financial information and enhances internal control activities. According to the audit risk model [2]:

$$PDR = \frac{AAR}{IR \times CR}$$

Where:

- PDR = planned detection risk
- AAR = acceptable audit risk
- IR = inherent risk
- CR = control risk

From the above risk model, as control risk decreases, the planned detection risk increases provided that the acceptable audit risk is certain. When the planned detection risk increases, the auditor can reduce costly audit tests and thus reduce the auditing fee. In addition, linking financial accounts to processes and controls and simplifying the access to information can make it easier for business unit managers and external auditors to evaluate compliance. "Auditors can come in and quickly see reports and evaluate effectiveness down to the account level," "Internal resources and external auditors can look at our financial accounts, then link them to processes associated with each, and then see the controls associated with the processes." [4]

Internally, the proposed ERP system reduces costs by eliminating redundancy and allowing companies to maintain the control objective in an efficient way. Compliance with SOX is a repetitious process and involves daily business operations. For such a process, an automated and real-time monitoring process undoubtedly is the best solution. The system also can support continuous inter-company reconciliations and posting of transactions to eliminate tedious manual reconciliations.

### CHALLENGES

The quality of information is very important to auditors. Before they express an opinion about a client's financial reports, auditors must ensure that the information generated through a client's system is reliable [8, 1]. This requires auditors to evaluate the adequacy of the controls surrounding a client's information processing systems and test them for errors and inconsistencies. In a conventional audit, auditors perform such an evaluation and testing only after a client's reporting period has ended and when the audit of financial reports begins. Even then, auditors do not examine one hundred percent of a client's system but select only a sample of transactions and examine them for errors and inconsistencies. In complex processing systems, a single error in processing could affect multiple records and the high transaction volume would make detection of these errors difficult [17].

The ERP model with a real-time monitoring function keeps standard and complete records of a business operation. XBRL-based records can greatly help auditors in audit tests, and give the auditors confidence about system reliability. The business process and control activities are monitored on a continuous basis; the external auditors can submit requests to the real-time monitoring system and better

evaluate companies' financial reports and internal controls. In previous models the auditor gathers information about a client's system electronically and through embedded monitoring tools evaluates the system reliability at regular intervals during the year [10, 8, 19]. Our model enables real-time monitoring at both auditor and company levels and allows the company to correct errors immediately.

The XBRL-based ERP system has continuous auditing functionality and enables the company to continuously comply with SOX in a cost-efficient way. If the company's related entities all use XBRL-formatted systems, auditors can most conveniently retrieve auditing evidence such as confirmation and documentation. While the proposed ERP system targets sustainable compliance with SOX, it also greatly improves companies' management in operating efficiency and internal control activities.

However, management needs to understand that the compliance efforts are ongoing efforts that require the management's continuous efforts to keep the process documentation updated. Companies should test whether the controls are working or not and should have evidence in place to document the control process. Standardized applications and the management's ongoing updating efforts are keys to making the ERP system active and useful.

### REFERENCES

1. Alles, M.G., Kogan, A., Vasarhelyi, M.A., 2002. Feasibility and economics of continuous assurance. *Auditing, A Journal of Practice and Theory* 21 (1), 123-138.
2. Arens, A.; Elder, R.; Beasley, M., 2006. Auditing and Assurance Services: An Integrated Approach. *Pearson Prentice Hall*.
3. Canadian Institute of Chartered Accountants and the American Institute of Certified Public Accountants. Continuous auditing, 1999. Toronto: *The Canadian Institute of Chartered Accountants*.
4. CFO Research Services, 2005. A Special Report on Process Improvement and Automation in the Age of Sarbanes-Oxley. *CFO Publishing Corp*. August.
5. Congress. The Sarbanes-Oxley Act of 2002, 2002. Pub. L. No. 107-204, 116 Stat. 745. July 30
6. Date, C.J., 1995. An Introduction to Stochastic Processes. *Addison-Wesley*, Reading, MA.

7. Davis, G.B., Weber, R., 1986. The impact of advanced computer systems on controls and audit procedures: A theory and empirical test. *Auditing, A Journal of Practice and Theory* 46, 1–28.
8. Elliott, R., 1997. Assurance service opportunities: Implications for academia. *Accounting Horizons* 11 (4), 61–74.
9. Elliott, R., 2002. Twenty-first century assurance. *Auditing, A Journal of Practice and Theory* (March), 139–146.
10. Groomer, S.M., Murthy, U.S., 1989. Continuous auditing of database applications: An embedded audit module approach. *Journal of Information Systems* 3, 53–69.
11. Groomer SM, Murthy US., 2003 Monitoring high volume transaction processing systems using a continuous sampling approach. *International Journal of Audit* 7:3– 19.
12. Halper, F.B., Snively, J., Vasarhelyi, M.A., 1992. The continuous audit process audit system: Knowledge engineering and representation. *EDPACS* (4), 15–22.
13. Li, Y., Roge, J., Rydl, L. & Crews, M., 2006. Information technology addresses transparency: the potential effects of XBRL on financial disclosure. *Issues in Information Systems*, vol. 7, #2, pp. 241-245.
14. Murthy, S. Uday and Groomer, S. Michael, 2004. A continuous auditing web services model for XML-based accounting systems. *International Journal of Accounting Information Systems* 5: 139– 163
15. Nearon, H. Bruce, 2005. Foundations in auditing and digital evidence. *The CPA Journal*. Vol. 75, No. 1, pp. 32-34.
16. Orman, L.V., 2001. Database audit and control strategies. *Information Technology and Management* 2 (1), 27–51.
17. Pathak, J., Chaouch, B., Sriram, S.R., 2005. Minimizing cost of continuous audit: Counting and time dependent strategies. *Journal of Accounting and Public Policy* 24: 61–75
18. Redman, T.L., 1992. Data Quality: Management and technology. *Bantam Books*.
19. Rezaee, A., Elam, R., Sharbatoghlie, A., 2001. Continuous auditing: Building automated auditing capability. *Auditing, A Journal of Practice and Theory* 21 (1), 147–163.
20. SEC 2003-66, 2003. “SEC Implements Internal Control Provisions of Sarbanes-Oxley Act, U.S. Securities and Exchange Commission, available at <http://www.sec.gov/news/press/2003-66.htm> , last accessed March 13, 2007.
21. United States Government Accountability Office, 2006. Report to the Committee on Small Business and Entrepreneurship, U.S. Senate. *Sarbanes-Oxley Act: Consideration of Key Principles Needed in Addressing Implementation for Smaller Public Companies*. GAO-06-361, April, 2006. Available at: <http://www.gao.gov/new.items/d06361.pdf> . Last accessed March 13, 2007.
22. Vasarhelyi, M., Halper, F.B., 1991. The continuous audit of online systems. *Auditing, A Journal of Practice and Theory* 19 (1), 110–125.
23. Vasarhelyi, M.A., Halper, F.B., Ezawa, K.J., 1991. The continuous process audit system: A UNIX based auditing tool. *The EDP Auditors Journal* 3, 85–91.
24. Vasarhelyi, M.A., Alles, M.G., Kogan, A., 2003. Principles of analytic monitoring for continuous assurance, Working Paper presented at Continuous Auditing Conference, *Texas A&M University*, College Station, TX. pp. 1–30.
25. Wang, R.Y., Storey, V.C., Firth, C.P., 1995. A framework for the analysis of data quality research. *IEEE Transactions on Knowledge and Data Engineering* 7 (4), 623–639.
26. Weber, R., 1988. EDP Auditing: Conceptual Foundations and Practices. *Prentice-Hall*, New Jersey.