JOURNAL OF EMERGING TECHNOLOGIES IN ACCOUNTING
Vol. 3
2006
pp. 61–80

Learning from WorldCom: Implications for Fraud Detection through Continuous Assurance

J. Randel Kuhn, Jr.
University of Central Florida

Steve G. Sutton
University of Central Florida
University of Melbourne

ABSTRACT: The recent rash of corporate frauds and malfeasance has intensified the focus on continuous assurance as a viable enterprise risk-management tool. In line with this focus, the current study revisits the WorldCom fraud and explores the feasibility of implementing continuous assurance over key-event-transaction data as a means of facilitating early detection of the main fraud activities that occurred. There are three main objectives of the research. The first is to examine the key methods of fraud executed by WorldCom's management in order to design a continuous assurance model that would have provided the analytic monitoring necessary for early detection of the fraudulent transactions. The second objective is to provide a blueprint for the integration of the prescribed continuous assurance model in an SAP environment as a means of demonstrating the feasibility of such a continuous assurance strategy. The third objective is to explore the complexity derived from the use of multiple-legacy systems as a means of articulating the resulting higher risk and the negative impact on the feasibility of continuous assurance. WorldCom forms the centerpiece of the research study based on the multiple fraud conditions and the coexistence of both SAP enterprise software and a myriad of legacy-system applications.

Keywords: continuous assurance; continuous auditing; continuous monitoring; SAP; enterprise systems; enterprise resource planning systems; enterprise risk management; WorldCom; fraud.

INTRODUCTION

With massive corporate failures sending shock waves throughout the stock markets, the last few years have seen a heightened focus on enterprise-risk management through stronger corporate governance, improved internal-control systems, more transparent corporate reporting, and broadening of the assurance scope to encompass all of these areas. Continuous assurance has accordingly received substantially greater attention

The authors thank participants at the 10th World Continuous Auditing and Reporting Symposium, and in particular Miklos Vasarhelyi, for their helpful comments and suggestions on an earlier version of this paper.

Corresponding author: Steve G. Sutton
Email: ssutton@bus.ucf.edu

as it is increasingly being viewed as a potential tool for helping minimize the risk of corporate fraud—particularly on the scale of what occurred at Enron, WorldCom, and Tyco.

Vasarhelyi (2005a) provides an examination of the Enron fraud and demonstrates how continuous assurance would have helped detect the fraud surrounding the special-purpose entities (SPEs) that were used to hide debt and prop up a positive outlook presented in the corporate financial statements. However, the continuous audit metrics that would have been most useful in detecting fraud at Enron are fairly specialized metrics that would have addressed a fairly unique fraud issue—and one that was reasonably understood by the auditors *a priori* to the fall of Enron.

WorldCom presents a very different situation, albeit a fraud of very similar magnitude. In 1999, revenue growth at WorldCom (the then second largest telecommunications company in the U.S.) began to slow quite dramatically, expenses became a steadily increasing percentage of revenue, and accordingly WorldCom's stock price began to drop. In an effort to meet earnings projections, management effected several fraudulent cost-reducing and revenue-enhancing mechanisms.

The purpose of this study is three-fold. The first objective is to examine the key methods of fraud utilized by the management at WorldCom as a basis for demonstrating the reasonableness by which a continuous assurance strategy could be formulated to detect such fraudulent behavior through the use of established principles of analytic monitoring (Groomer and Murthy 1989; Vasarhelyi and Halper 1991; Kogan et al. 1999; Woodroof and Searcy 2001; Vasarhelyi et al. 2004). The study focuses on a set of analytics that are not complex, but rather demonstrate the ease at which the fraudulent behavior could have been detected through the application of continuous assurance. As SAP implementations are highly prevalent in industry, the second objective is to clearly articulate a design for integrating the prescribed continuous assurance strategy with an SAP-based enterprise system similar to WorldCom's. The third objective is to explore the barriers to continuous assurance applications that arise in highly complex system environments by illustrating how the myriad of loosely connected legacy systems under WorldCom's enterprise software created an intractable monitoring problem that would have limited the completeness of any continuous monitoring system.

The demonstration of how a reasonable and practical implementation of continuous assurance would have detected a major fraud is a critical next step in the support of efforts to make continuous assurance a frequently used audit tool. The system detailed is conceptually simple and readily implementable in an enterprise systems-driven environment. On the other hand, the complexities of the continued use of widespread, independent legacy systems creates an intractable control and monitoring problem and should similarly be recognized as a major risk factor in any financial statement audit—not just for future continuous audit implementations. In total, a contingency model exists whereby the complete support of business processes through standardized enterprise systems software presents a feasible environment for continuous assurance implementation, but as the number of legacy systems feeding data into the enterprise software increases, the complexity of implementing continuous assurance escalates rapidly to the point of reaching infeasibility rather quickly.

The research presented in this paper contributes to the growth of continuous assurance research in three important ways. First, it provides a detailed understanding of how continuous assurance techniques that have been explored in the literature can effectively identify fraud in a known fraud situation. Second, it moves the literature on continuous assurance models forward by addressing the complexities of implementation within a standardized enterprise software environment (e.g., SAP). Third, it addresses the realities and risks associated with large numbers of disparate legacy systems.

The remainder of the paper consists of four major sections. The first section details the nature of the underlying fraud techniques used by WorldCom's management and describes a set of analytic monitoring features that would have detected the fraud. The second section addresses the implementation of the analytic monitoring features in an SAP enterprise software system such as that used by WorldCom. The third section addresses where the continuous monitoring system would break down at WorldCom due to the widespread use of disparate billing systems that continued to exist in legacy form without directly feeding the data into the central SAP system. The fourth and final section summarizes the implications of the research and outlines opportunities for future research.

DETECTING A WORLDCOM-TYPE FRAUD THROUGH CONTINUOUS AUDITING

Businessmen Murray Waldron and William Recktor established Long Distance Discount Service (LDDS) in 1983 as a reseller of long distance services. Early investor Bernard Ebbers, a former motel chain owner from Mississippi, became the chief executive in 1985 and took the company public in 1989. LDDS officially renamed itself WorldCom in 1995.

Throughout the 1990s WorldCom grew tremendously through the acquisition of over 60 communication companies primarily purchased with WorldCom stock. The $37 billion merger with MCI in 1998 represented the largest merger in history at that point in time. The merged entity became the second largest long distance carrier (1998–2002) and controlled over half of all Internet traffic in the United States and half the emails worldwide. By 2001, WorldCom owned one-third of all the data cables in the United States.

United States and European regulators blocked a subsequent merger attempt by WorldCom and Sprint in 2000. The failed merger signified the beginning of the end for WorldCom. As long-distance rates and revenue declined, the accumulation of debt and expenses placed a strain on the financial health of the company, threatening WorldCom's ability to meet key-performance indicators and earnings projections.

Analysts and observers within the Telecom industry typically focus on the line cost expenditure-to-revenue (E/R) ratio as a critical performance indicator. WorldCom management touted a lower E/R ratio (42 percent) than their competitors and consistently struggled to maintain that level during the fraud years (Kaplan and Kiron 2004). To meet analysts' expectations, management manipulated financial information to increase the appearance of revenue growth, cost reduction, and overall profit. The end result was the largest corporate fraud in U.S. history at $11 billion.

WorldCom management utilized various techniques to mask their financial condition, but four in particular drove the major material misstatements: (1) categorizing operating expenses as capital expenditures, (2) reclassifying the value of acquired MCI assets as goodwill, (3) including future expenses in write-downs of acquired assets, and (4) manipulating bad debt reserve calculations. The cumulative impact of the four techniques resulted in enhanced perceptions of financial position and viability by reducing the key E/R ratio and boosting overall net income from operations (see Table 1 for a summary of the effects). Each of these four techniques is explored in further detail.

WorldCom began classifying operating expenses as long-term capital investments in 2000. Generally accepted accounting principles (GAAP) dictate that operating expenses must be immediately recognized in the period incurred, unlike capital expenditures, which

TABLE 1

Fraud Scheme	Financial Effects			Cite
	Expenses	Assets	E/R Ratio	
Categorizing operating expenses as capital expenditures	↓	↑	↓	Feder and Schiesel (2002)
Reducing the book value of acquired MCI assets and simultaneously increasing goodwill for a balancing amount	↓	Balanced Effect	—	Eichenwald (2002)
Including future expenses in write-downs of acquired assets	↓	↓	↓	Eichenwald (2002)
Revising bad debt reserve calculations to boost the valuation of receivables that were subsequently factored	↓	↑	—	Sender (2002); Feder and Schiesel (2002)

may be capitalized as assets and depreciated over their useful life.[1] Deferment of these costs artificially inflated reported net income and misled financial statement users. The payments to lease phone network lines from other companies (i.e., allowing access to their networks) are commonly referred to as “line costs” and represent the numerator in the E/R ratio. The fraudulent capital expenditures resulted from manual reclassification of existing operating expense account balances and inappropriate recording of future line-cost transactions. As an example, the first quarter 10-Q report filed with the SEC in 2001 reported $4.1 billion of line costs and revenue of $9.8 billion resulting in an E/R ratio of 42 percent. Restated financial statements (i.e., post-fraud) disclosed actual line costs of $4.9 billion. The initial reclassification by WorldCom of $771 million of line costs to capital expenditures was used to reduce the E/R ratio from 50 percent back to the desired level of 42 percent (Kaplan and Kiron 2004).

The MCI merger provided WorldCom another opportunity to defer expenses. Management reduced the book value of MCI assets by several billion dollars and simultaneously increased the value of goodwill by a balancing amount. The related goodwill would be amortized over a significantly longer period than that for normal asset depreciation based on estimated useful lives of the respective assets. At the time of the fraud, GAAP permitted amortization of goodwill over 40 years. This scheme enabled WorldCom to spread the cost of the MCI assets over a longer period of time by recognizing a smaller amount of expense each year and overstating net income.

In addition to the aforementioned MCI goodwill scheme, WorldCom employed fraudulent accounting to numerous other corporate acquisitions. The company wrote-down millions of dollars in acquired entities’ assets resulting in excess charges against current earnings—generally referred to in the earnings management literature as “taking a big bath” (Healy 1985) by absorbing costs at one point where they are not unexpected nor predictable by the markets in order to improve future financial reports. The excess charges related to costs other than those related to the assets that were being written down. The net effect

[1] The Financial Accounting Standards Board (FASB) Concept Statement No. 5, *Recognition and Measurement in Financial Statements of Business Enterprises*, discusses when various types of expenses should be recognized. FASB Concept Statement No. 6, *Elements of Financial Statements*, further defines the characteristics of expenses and assets and treatment of related costs.

was to create larger losses for the current quarter (i.e., the big bath) in order to improve the picture presented through financial reports in future quarters. WorldCom wished to create the false impression that expenses were declining over time in relation to revenue (i.e., reducing the E/R ratio and increasing net income from operations). Users of the statements were essentially deceived into believing there would be better performance in future periods, maintaining upward pressure on the value of WorldCom's stock.

From 1998 to 2000, WorldCom aggressively managed accounts receivable assumptions and related bad debt reserves. When a company extends credit to a customer with the promise by the customer to pay in the future, invariably a portion of these customers will ultimately not pay all or part of their bill. An estimate of the portion of receivables that will not ultimately be collected must be derived and a related expense accrued on the financial statements. Companies estimate the amount that should be expensed as uncollectible on the income statement and the net amount of accounts receivable (i.e., gross accounts receivable less the allowance for uncollectible accounts) to report on the balance sheet. Altering the percentage of accounts receivable in the estimation of the uncollectible portion directly impacts the bad debt expense reported on the income statement and the reserve amount netted against gross accounts receivable on the balance sheet.

WorldCom's revenue and total accounts receivable decreased $3.9 billion and $1.95 billion, respectively, in 2001. As a percentage of total accounts receivable, the allowance for doubtful accounts (i.e., the reserve) decreased from 18.35 percent in 2000 to 16.98 percent in 2001. Applying the same reserve calculation as utilized in the previous year, earnings would have decreased even further by another $87 million. Either the company drastically improved collection efficiency or under-reserved thus artificially inflating both reported revenue and the value of receivables to be factored in the future.[2] The latter seems most likely given that the company recorded a $322 million adjustment to write-off additional bad debt in 2002, restated the 2001 allowance account by an increase of $751 million, and ultimately filed for bankruptcy protection on July 21, 2002.

The methods of manipulating financial information described in the preceding paragraphs may not comprise all the ways in which WorldCom committed fraud. The four do represent the core techniques employed by WorldCom that ultimately resulted in the most significant adverse consequences. The challenge for the auditor is to identify a feasible means for detecting such behavior in order to avoid a replication of the WorldCom fraud at another company in the future.

Auditor Detection of Fraud

Extant research portrays a rather grim picture of the ability of auditors to detect fraud. The participants in Pincus' experimental study (1989) ironically identified more manipulated fraud situations when not using a "red flag" checklist (as is commonly used by the major firms) than when the checklist was available. Hackenbrack (1993) found auditors had differences of opinions as to the level of fraud risk associated with specific "red flag" indicators. Client experiences (particularly client size) heavily influenced varying perceptions of risk. Graham and Bedard (2003) found that fraud detection is further complicated by the high proportion of audit clients that exhibit one or more fraud risk factors while planned and performed fraud assessments generally fail to fully address the risk. Overall, auditors exhibit difficulty in consistently assessing the risk of material misstatement of financial statements due to fraudulent reporting.

[2] Factoring accounts receivable (i.e., selling) at higher values results in increased reported income based on faulty assumptions.

In an effort to enhance auditor performance in fraud risk assessment, Eining et al. (1990) created an expert system and subsequently tested auditor performance with the system against use of a fraud risk-factor checklist or a logit predictive model (Eining et al. 1997). The expert system outperformed both alternative decision aids. This finding is somewhat encouraging from a continuous audit perspective as expert system technology could easily be integrated into a Continuous assurance Analyzer component as discussed in the following subsection.

Continuous Assurance Framework

The traditional attestation framework contains inherent flaws hindering timely and relevant assurance reporting (Vasarhelyi and Halper 1991). Auditors typically receive data from clients that present only a ‘‘snapshot’’ of the financial reporting system. The external audit rarely provides information facilitating timely decisions for management, creditors, investors, or auditors. While auditors increasingly work to spread the audit work throughout the year, the bulk of business process and information technology (IT) controls testing, as well as high-level financial analytics, are still conducted during third quarter interim testing prior to the detailed end-of-year substantive-based test procedures. The result is a concentration of activity during a short timeframe, making time very precious.[3] Any delay caused by the client (intentional or unintentional) or the auditor due to poor planning/estimation can cause the auditor to reevaluate planned audit procedures and consider reducing the level of auditing. Continuous auditing represents a means to alleviate this time pressure.

In a joint study performed by the Canadian Institute of Chartered Accountants and American Institute of Certified Public Accountants, continuous auditing is defined as ‘‘a methodology for issuing audit reports simultaneously with, or a short period of time after, the occurrence of the relevant events’’ (CICA/AICPA 1999). The continuous auditing movement over time has refined the related terminology and now recognizes two distinct types of continuous monitoring, ‘‘continuous auditing’’ and ‘‘continuous assurance,’’ defined by Alles et al. (2002, 128) as:

> [Continuous auditing] is best described as the application of modern information technologies to the standard audit products ... Continuous auditing is another step in the path of the evolution of the financial audit from manual to systems-based methods ... By contrast, continuous assurance sees continuous auditing as only a subset of a much wider range of new, nonstatutory products and services that will be made possible by these technologies.

Consistent with the description by Alles et al. (2002), the remainder of this paper will focus on the technique of continuous auditing as a tool in a continuous assurance framework.

The Continuous Process Auditing Methodology (CPAM) put forth by Vasarhelyi and Halper (1991) offers a framework from which to explore the development and refinement of a continuous auditing approach. In their methodology, transactional and system data are monitored and analyzed continuously based on a rule-set predefined by the auditors in the continuous audit application. Exceptions to the rules trigger alarms that automatically notify the auditors of potential irregularities. The nature of audit work transcends from primarily a substantive-based test of details approach to a focus on auditing by exception.

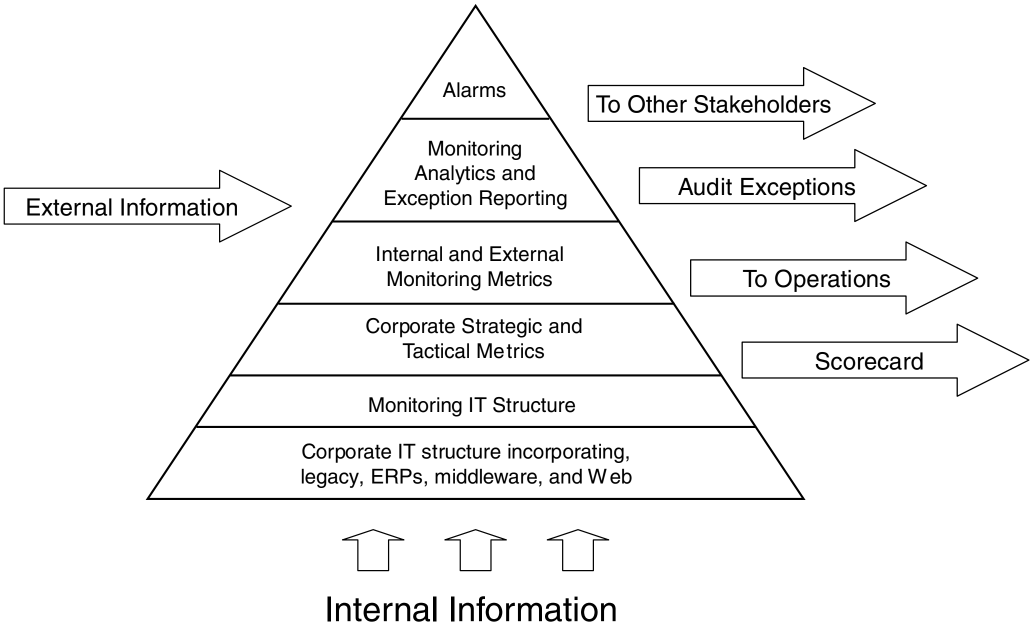
[3] Substantive audit procedures are activities performed by the auditor that gather evidence to test the completeness, validity, and/or accuracy of account balances and underlying classes of transactions. Tests of detail represent the collection of certain types of evidence (e.g. vouching supporting documentation, physical examination of assets, recalculation of estimates and entries, third party confirmation of assets/liabilities, inquiry of client employees, etc.).

Figure 1 describes a view of corporate monitoring processes from an assurance perspective (Vasarhelyi 2005b). Corporate information technologies (e.g., legacy, enterprise systems, middleware, and web-based systems) provide the monitoring structure that facilitates measurement functions such as strategic and tactical metrics, internal/external monitoring metrics, and monitoring analytics. This combination of technologies and programmed metrics provides a basis for reporting key-performance indicators, corporate scorecards, audit exceptions/alarms, and external reports (Vasarhelyi 2005b).

Continuous auditing presents opportunities to increase the effectiveness and efficiency of the attestation function. The capture of data on a continuous, real-time basis facilitates immediate identification of exceptions, generation of alarms, and presumably prompt action by the auditor. Auditors can increase the coverage of testing by obtaining data throughout the entire year and comparing to previous periods, industry averages, and knowledge gleaned from the firm's client portfolio for variations in trends among the data with minimal effort. Automation allows the auditor to conduct test procedures embedded into the monitoring analytics at any time as opposed to just traditional interim and year-end periods. Computer-processed test procedures are also executed faster and more accurately than manual procedures. Continuous auditing solves many of the deficiencies in the traditional audit framework while increasing the overall quality of the audit.

The process of continuous auditing represents a sophisticated analytic review technique permitting auditors to improve the focus and scope of the audit. In the CPAM approach, Vasarhelyi and Halper (1991) outline the foundation for continuous auditing as essentially

FIGURE 1
Monitoring Framework


Alarms
Monitoring Analytics and Exception Reporting
Internal and External Monitoring Metrics
Corporate Strategic and Tactical Metrics
Monitoring IT Structure
Corporate IT structure incorporating, legacy, ERPs, middleware, and Web
External Information
To Other Stakeholders
Audit Exceptions
To Operations
Scorecard
Internal Information

Replicated from Vasarhelyi (2005b).

three phases: (1) Measurement, (2) Monitoring, and (3) Analysis. Measurement consists of key management reports (e.g., financial statements, security settings) from which metrics are derived for comparison to standards. During the monitoring phase, the audit system performs constant comparison of metrics to the standards programmed into the system (i.e., analytics) and triggers alarms to notify auditors of any inconsistencies. Vasarhelyi and Halper (1991, 117) define analytics as ‘‘functional (natural flow), logical (key interaction), and empirical (e.g., it has been observed that ...) relationships among metrics’’ that can be derived from auditor, management, or user experience and historical data in the system. In the final phase, the auditors review the nature of the alarms and investigate as appropriate.

Vasarhelyi et al. (2004) further expand on the theme of continuous auditing as an analytic tool. They contend that market demand will shift assurance requirements away from the traditional ‘‘*ex post* evaluation’’ to a more ‘‘close-to-the event’’ review. The new role of auditors will be more invasive as they monitor day-to-day business operations through the use of technology and auditing by exception. To distinguish from the traditional auditor role, Vasarhelyi et al. (2004) refer to the new process as ‘‘analytic monitoring.’’

The new assurance technologies described by Vasarhelyi et al. (2004) allow analytic monitors to observe events as they transpire, trigger alarms when exceptions occur, drill down to transactional detail, integrate data across multiple and distinct processes, and perform repeated tests at minimal cost. Vasarhelyi et al. (2004) also examine several tools that underlie analytic monitoring such as continuity equations, tagging data accuracy, time series analysis, dynamic reconciliation of accounts, data taps, confirmatory extranets, and invisible tags. These analytic tools could have been strategically implemented at WorldCom, facilitating early identification of fraudulent activity.

Recent legislation and reporting trends, such as the Sarbanes-Oxley Act of 2002 (SOX) and initiatives for continuous disclosure of financial information, provide greater incentives for the development and use of continuous assurance in the financial reporting environment. Section 404 of SOX requires external auditor evaluation of the effectiveness of internal controls over financial reporting. Continuous assurance of key technology-related controls can be an integral component of the auditor’s overall 404-compliance audit with the results used as evidence to assist in the determination of the auditor’s opinion (e.g., Alles et al. 2006). SOX also speaks to the need for continuous financial reporting which is only feasible if continuous assurance can be provided over system’s reliability and through event transaction monitoring. Continuous assurance necessitates activities that monitor both internal controls and transaction processing.

Continuous Assurance to Detect a WorldCom Fraud

The accounting measurement rules applied to business transactions at WorldCom defied Generally Accepted Accounting Principles (GAAP). For instance, WorldCom management inappropriately reclassified previously recorded operating expenses and future expenses as capital expenditures. Incorporating measurement rules into the continuous assurance rule-set can be difficult due to the ambiguity in formulation as prescribed by GAAP and the complexity and variety of modern business transactions (Vasarhelyi et al. 2004). Even with such difficulties, some very basic analytic procedures programmed into the rule-set will trigger alarms to auditors identifying potential fraudulent activities similar to those at WorldCom.

Continuous flow of information facilitates the use of time series analyses to create points of reference based on historical data for comparison with current data. In addition, the continuous auditing rule-set can integrate industry norms and trends derived either from auditor research or information provided by digital agents (Woodroof and Searcy 2001).

Consider WorldCom's fraudulent capital expenditures. Comparison of historical balances and ratios of operating expenses and capital expenditures in relation to current balances and industry norms/trends trigger alarms to auditors. Shifts in account balances from operating expenses to capital expenditures, similar to the significant reclassification entries at WorldCom, would automatically trigger alerts to the auditors. Similarly, WorldCom posted fraudulent entries totaling several billion dollars associated with the MCI merger by writing down assets and transferring costs to goodwill. Analytic monitoring would again identify similar entries with appropriate rule-set configurations that flag the simultaneous decrease of assets and increase in goodwill (i.e., balanced entries).

WorldCom committed fraudulent acts related to other acquisitions by including future operating expenses in the write-down of acquired assets. While the industry experienced diminishing operating profit margins due to ever-decreasing prices and increased competition, WorldCom showed increasing profit margins each quarter. Analytic monitoring embedded in the continuous assurance application could identify instances where key financial ratios, such as operating expenses as a percentage of total revenue, deviate from industry trends.

The final WorldCom fraud scheme pertained to manipulation of bad debt reserves. Bad debt reserves can be either over-funded (i.e., creating a ''cookie jar'' effect that allows management to later ''dip into'' the reserve to increase earnings in subsequent years) or under-funded (i.e., artificially inflating the short-term value of accounts receivable and earnings). WorldCom appears to have under-funded their reserves during the years of fraudulent activity. Implementation of standard analytic monitoring in the continuous assurance system would facilitate analysis of bad debt reserve calculations for appropriateness. Analytic monitoring could draw from industry averages, creating metrics in the rule-set that use industry trend data in combination with the client's historical accounts receivable collection information to assess the reasonableness of current reserve calculations.

The fraudulent activities conducted at WorldCom to increase the appearance of current profits and future earnings growth provide a solid foundation for demonstrating how continuous assurance could be used to (1) increase the possibility of detecting fraud and (2) enhance the timeliness of fraud detection. Incorporating analytic monitoring into the overall assurance framework creates a richer ''suite'' of techniques and tools than are currently available in traditional audit approaches. The alerts generated from the analytics assist in directing the auditor's attention to potential high-risk areas that may otherwise go undetected or only be recognized very late in the audit process. The system of analytics underlying the alerts provides the auditor with the opportunity to detect potentially fraudulent behavior much earlier in the fraud process through continuous monitoring for unanticipated fluctuations. Ultimately the auditor must still act on the alerts for the detection to lead to effective auditing. If the auditor ignores the alert or fails to adequately explore a problem area, as in the WorldCom fraud, then the continuous assurance system may still fail.

IMPLEMENTING CONTINUOUS ASSURANCE METRICS IN AN SAP ENVIRONMENT

The advent of Enterprise Resource Planning (ERP) systems has allowed organizations to seamlessly integrate and automate business processes to achieve real-time information flow. As a by-product, the integrated platform provides an enabler for the use of continuous assurance procedures to monitor and report companies' financial condition on a more timely basis than traditional audits.

To date, the continuous assurance literature has primarily focused on the concepts and methodologies of continuous assurance. At this point in this research study, the focus shifts to the development of an instantiation of analytic monitors in an SAP R/3-based enterprise system. The objective is to illustrate the application of existing theoretical work into a standardized software environment and to demonstrate how very basic analytical procedures configured in a continuous assurance application can uncover the types of fraud committed at WorldCom.

System Architecture for Continuous Monitoring

Two contending system architecture models exist in the extant continuous assurance literature, the monitoring and control layer (MCL) and the embedded audit module (EAM). MCL utilizes an independent server owned and controlled by the auditor that receives regularly scheduled data interfaces (read-only) from the client's enterprise system (Vasarhelyi et al. 2004). Application software configured on the auditor's server, referred to as the CA Analyzer by Alles et al. (2006), processes the data against the predefined rule-set flagging and notifying auditors of any deviations. MCL monitors on a near real-time basis. Alternatively, EAM functionality is embedded into the client's system and operates in real-time notifying auditors instantaneously (Groomer and Murthy 1989). Each model offers distinct advantages.

Alles et al. (2006) compare the two traditional approaches, ultimately choosing MCL for a Siemens pilot project on continuous monitoring of business process controls. Assessing the SAP environment at Siemens Corporation, Alles et al. (2006) identify several key advantages of MCL, including: (1) increased control over the system (i.e., data integrity and security), (2) minimal impact on the performance of the client's system, (3) less required cooperation from client personnel, and (4) reusability of core system functionality that reduces the costs of implementing additional continuous audit environments. Control over the configuration, operation, and maintenance of the continuous assurance application by the auditors helps mitigate concerns of independence and eliminate the risk of client personnel manipulating the continuous assurance system to avoid fraud detection. System performance weighed heavily on Alles et al.'s (2006) decision when selecting a continuous assurance approach. SAP requires significant resources along with diligent capacity management to operate. Incorporating third-party bolt-on applications to operate concurrently with normal SAP processing historically has had severe adverse effects on performance. Simply activating the audit logging function native to SAP can critically impede normal processing.

Groomer and Murthy (2003) recently developed a modified version of the EAM approach that utilizes continuous sampling procedures (CSP) to work in conjunction with embedded procedures. CSP procedures sample a portion of online transactions rather than the complete population monitored by EAM. This strategy allows EAM functionality to be automatically switched to a CSP mode based on preset criteria designed to alleviate system performance issues. Implementing embedded analytics, even at this modified level of activity, still risks severely affecting system performance. Concerns over detrimental performance effects make MCL the model of choice in the research analysis being explored in this study.

SAP R/3 operates in a client-server environment and the architecture consists of three tiers defined as the presentation, application, and database layers with each operating on a separate computer. The presentation layer provides the graphical interface to the user while the application layer acts as the "engine" processing information contained in the database layer.

The key architectural design question becomes whether to access the enterprise information via the application layer or directly from the database. Due to the size and complexity of SAP databases, Alles et al. (2006) elected to extract data from the application layer using application program interfaces, termed BAPIs in SAP terminology. BAPIs are typically supported by system vendors and well documented—providing a practical approach. This approach works well with the Siemens prototype where control processes are largely embedded within the application layer.

Given the focus of this research study on financial statement information, the rationale for aggregating data through the application layer no longer exists. For the required analytics in the WorldCom example, the focus is on analyzing consolidated financial accounting information from an analytic perspective. This requires obtaining transaction and account detail from the SAP general ledger that resides in two SAP tables: the GLPCT (summary table of account balances) and the GLPCA (individual transaction data). Extracting all necessary data from two tables within the database layer significantly reduces the complexity faced by Alles et al. (2006), offering a more simplistic approach than accessing data through the application layer via BAPIs.

The CA Analyzer operates external to the SAP application and performs test procedures against extracted data residing in a relational database. To obtain the necessary data, an extractor program executes a remote function call (RFC) requesting access to SAP. RFC is a standard programming interface that can be used to send and receive data. The RFC connection must be given a unique SAP user ID and password with permission to display tables (authorization object S_TABU_DIS) and to execute an RFC (authorization object S_RFC). Table display access can be further restricted to view only GLPCT and GLPCA.

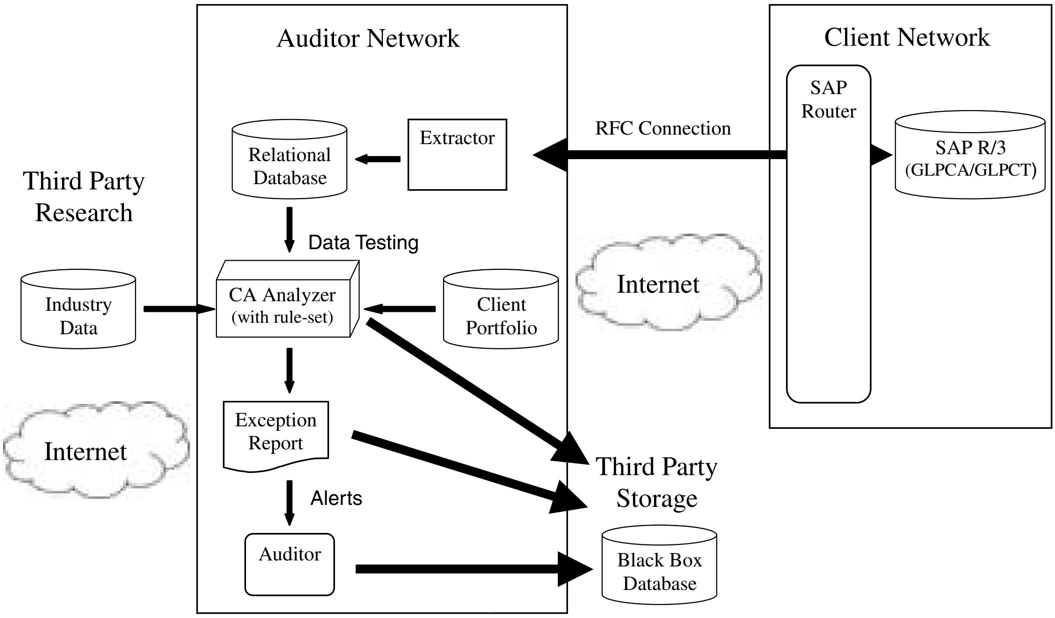
SAP software provides an application-level gateway program called SAProuter that serves as a proxy controlling communication with other systems (i.e., access to and from SAP). SAProuter contains a routing table that defines the IP addresses for approved external connections. If utilized, SAProuter can provide an additional layer of security for interaction between the RFC and the client's SAP environment. The auditor therefore must coordinate with the client to establish and configure user access rights for the RFC and connection permission in the SAProuter table. Figure 2 illustrates the interaction between the external program called an extractor that executes an RFC connection to SAP and is validated by SAProuter.

Integrating MCL and SAP

The primary task of a continuous assurance application is to identify instances where the observed data deviates from the predefined rule-set in the CA Analyzer. The application must automatically generate alarms notifying the auditors of critical exceptions. Figure 2 illustrates the process structure and data flow utilized in the continuous assurance application documented in this study. The structure includes an SAP R/3 ERP system, an extractor program, a relational database, industry data, client portfolio data, a CA Analyzer with workflow management to generate alarms and automatic email notification to the auditors, and a "black box log file."

The CA Analyzer receives data from three data sources: (1) the relational database containing extracted information from the client financial system, (2) industry data provided by a third party research organization, and (3) client portfolio data containing key risk factors. Client portfolio is generally readily available as many public accounting firms have developed firm-specific applications for client acceptance and continuance decisions that include detailed analytics tied to firm risk models. As examples, Bell et al. (2002) discuss the implementation of KPMG's KRisk^{SM} system, and Winograd et al. (2000) discuss the implementation of PricewaterhouseCoopers' FRISK system—both designed to facilitate the client acceptance risk-assessment process. In these systems, the risk-assessment data can

FIGURE 2
Continuous Audit Data Flow
(MCL⟵⟶SAP)



"feed forward" into the planning, testing, and review phases of the audit. Likewise, interfaces to the CA Analyzer from the client portfolio application can continually update the rule-set configuration within the CA analyzer with client-specific risk factors.

The "black box log file," as recommended by Alles et al. (2004), provides a mechanism for recording and retaining the continuous audit evidence allowing tertiary monitoring of the auditor (i.e., audit of the auditor). The maintenance of the monitoring data provides a motivation for the auditor to explore risks highlighted in alerts rather than ignoring them.

The illustration herein will address the four previously discussed fraudulent schemes employed at WorldCom by demonstrating the manner in which a properly configured continuous auditing application would identify the issues in a timely manner. For purposes of the illustration, assume a single SAP instance containing the general ledger account balances and consolidated financial information (i.e., the information reported to the SEC and investors) versus a company operating multiple SAP applications for various business processes/units.

The key factors dictating the type of relational database required for the continuous assurance structure include the size of the extraction, number of ERP systems evaluated, length of retention of the data, and frequency of downloads (Alles et al. 2006). For prototyping purposes, the Siemens proof-of-concept stored the extracted data in an MS Access database. However, the team recognized that a robust relational database with database management and support capabilities (e.g., Oracle or MS SQL Server) would be required in a production environment.

The key component of the continuous assurance system entails the configuration and operation of the CA Analyzer. The rule-set defined in the application determines the identification of exceptions and subsequent auditor notification. The rule-set is the driving force enabling monitoring.

Alles et al. (2006) developed a CA Analyzer in Visual Basic for the Siemens project as a test environment to evaluate the technical research questions regarding continuous assurance. The Siemans project focused on continuous monitoring of business process controls. The configuration of the CA Analyzer addressed the SAP controls as defined in the Siemens IT audit plans (e.g., comparison of password and system parameter settings to best practice standards).

The focus of this paper differs from Alles et al. (2006) in the nature of the analytic monitoring to be performed by the CA Analyzer. The Siemens project standardized and automated certain tasks and procedures within existing audit programs developed by the internal IT audit department to review SAP business process controls and system parameter settings replicable across hundreds of SAP instances. The objective of the approach developed herein concentrates on developing an automated mechanism for external auditors to detect financial irregularities and material misstatements of the financial statements in a timely fashion through substantive-based audit procedures. The illustration in this research is alternatively focused on how WorldCom management conducted financial fraud and the rule-set configuration necessary to detect such behavior. To reiterate, the key WorldCom fraudulent activities included inappropriate reclassification of operating expenses as capital expenditures, reclassification of acquired MCI assets as goodwill, inclusion of future company operating expenses in the write-down of acquired assets, and manipulation of bad debt reserve calculations. The rule-set developed in this study focuses on these specific acts of fraud. Development of the full set of analytics that would be desirable for complete monitoring is beyond the scope of this study.

Identification of material reclassifications of operating expenses as capital expenditures could occur through several monitoring analytics. The CA Analyzer can store multiple years worth of financial data (i.e., general ledger account balances) and compare the company's historical ratios of operating expenses and capital expenditures to sales revenue. A decline in the proportion of operating expenses to sales revenue and corresponding increase in the ratio of capital expenditures to sales revenue exceeding a configured threshold would trigger one alarm. Related industry and firm risk data can also be incorporated into the CA Analyzer to facilitate variations of the metric. An alert is communicated if the company's ratios differ substantially from expected ranges.

Analytic monitoring to identify inappropriate reclassifications (based on industry averages) can be configured as:

> IF the operating expenses to sales ratio is $>$ 2% below .93 AND the capital expenditures to sales ratio is $>$ 5% above .15, THEN create an alert.

WorldCom's 2001 operating to sales and capital expenditures to sales ratios were .90 and .22, respectively, and exceeded the sample thresholds by $946 million and $585 million, respectively.

WorldCom wrote down assets acquired in the MCI merger transferring the cost to goodwill in the same amount. The sheer magnitude of the entries, in and of themselves, should raise concern. All material journal entries, regardless of account, should be examined by the auditors. The auditors can configure the rule-set to identify journal entries above a certain dollar threshold to trigger such an alert. More specific to the assets and goodwill account, the CA Analyzer can contain logic identifying significant changes in key account balances over a short time period. The excessive growth of WorldCom through merger and acquisition, asset additions, write-downs, and purchased goodwill accounts warranted special attention. The CA Analyzer can be configured to focus attention on accounts containing higher audit risk.

A sample monitoring analytic to identify inappropriate asset reclassifications to goodwill can be configured as:

> IF the property, plant, and equipment and goodwill account balances increase or decrease by $>$ .01% from the last extraction, THEN create an alert.

WorldCom's goodwill balance at the 2001 year-end was $50.5 billion. The 01 percent threshold equated to a change of $5 million. Actual change from the previous year was $3.9 billion which would trigger an alert for the group of entries during 2001 that reclassified MCI assets to goodwill.

The acquisition activities of WorldCom resulted in additional fraudulent acts. The company wrote-down assets and in doing so, included future company operating expenses. This allowed the E/R ratio (i.e., line cost expenditure/revenue) to remain steady at 42 percent over a sustained period. The telecommunications industry, as a whole, experienced lesser margins during the same period as a result of steadily increasing E/R ratios (i.e., the industry average was 50 percent—see Kaplan and Kiron [2004]). Entering key industry indicators into the CA Analyzer and configuring the application to identify significant deviations from those trends, would flag such an irregularity. A number of vendors such as the United States Telecom Association, Moody's, BizMiner, etc. sell key telecom industry-specific information such as financial statement line items and key ratios, historical and forecasted growth, specific sector analyses, and other information that auditors could automatically load into the underlying database of the CA Analyzer. Comparison of current line cost expenditures and revenues to industry trend ratios by the CA Analyzer would have raised alerts.

Analytic monitoring to identify the inappropriate inclusion of future expenses in current write-downs of acquired assets can be configured to compare the trend of the client's E/R ratio over both a five-year period and the course of the most recent 12 months to that of the industry.

> IF the slope of the trend (where $x =$ time period, $y =$ E/R ratio) falls below that of the industry trend by $>$ 1%, THEN create an alert.

As previously noted, the industry experienced progressively worse E/R ratios (i.e., positive slope) whereas WorldCom repeatedly reported constant E/R ratios (i.e., a flat trend line with zero slope). The difference in slope between the industry and WorldCom would have created an alert.

Historically, bad debt reserve calculations represent an area susceptible to accounting fraud. The reserves can be manipulated in either direction by the company's management, expensing more bad debt in good times and less in leaner periods. During the years of fraudulent activity, WorldCom exhibited behavior consistent with under-funding of bad debt reserves in an apparent effort to lower expenses and inflate receivables. Industry related data integrated into key metrics within the CA Analyzer, along with logic to perform comparisons of current bad debt ratios to historical estimations and actual expenses incurred, would have triggered an alert.

Analytic monitoring to identify bad debt reserves manipulation could be configured as:

> IF the change in the ratio of bad debt allowance to total accounts receivable is $>$ 1% below last month's figure, THEN create an alert.

The bad debt reserve estimate dropped by 1.4 percent in 2001 from the prior year ‘‘saving’’ the company $87 million in bad debt expense. An alert to the auditors would have been created when the reserve calculation dropped below the threshold.

As shown in the Siemens project (Alles et al. 2006) and our systems design for financial statement information monitoring, the MCL strategy for continuous assurance can be effectively implemented in an SAP environment while minimizing the impact on the system and its users. Automation of common analytical procedures through the configuration of the CA Analyzer rule-set offers a valuable tool to quickly process and analyze the extensive volume of data typically residing in a major ERP system. The external auditor has the additional benefit that data necessary for financial transaction and account balances monitoring can be extracted directly from the SAP database, precluding the client from monitoring the specific information being examined whereby the auditor’s tests might be circumvented. The auditor also avoids any manipulations of the client’s system, thereby alleviating the independence concerns that have been raised in relation to continuous assurance. In summary, the technology exists to successfully design, implement, and operate an effective continuous assurance application within a standard enterprise systems environment.

INTEGRATION RISKS IN DISPERSED SYSTEM ENVIRONMENTS

The technological feasibility of continuous assurance systems requires financial information to be recorded and stored in electronic form and the availability of adequate network architecture to facilitate continuous remote access to the information (Kogan et al. 1999). Nearly all companies utilize such technology to capture and record information for financial reporting. ERP systems facilitate the accumulation of enterprise information from various business processes into a single application, storing the massive amounts of data in a single database. Current internet technology now provides the capability to directly access enterprise data easier, quicker, and cheaper. Readily accessible financial data enables feasible implementation of continuous assurance procedures.

Issues arise, however, when companies employ disparate systems built on various technological foundations (i.e., legacy systems). The multiple platforms, assorted data formats, and varied interfaces to the financial reporting system complicate the design, implementation, execution, and maintenance of continuous assurance applications. To effectively monitor, continuous assurance applications must access or receive information from all the various applications processing data that materially impact the financial statements. Yet, many legacy systems have been designed to be standalone systems with limited networking capabilities.

The WorldCom scandal discussed throughout this paper also illustrates the challenges to implementing continuous assurance applications. As previously mentioned, WorldCom produced their financial statements from information contained in an SAP R/3 environment. The continuous assurance procedures identified in the previous section that may have recognized the more prominent fraudulent activities focused on analyzing data contained in the SAP general ledger module and sub-ledgers. If WorldCom processed all financial data within the SAP environment, the CA Analyzer configuration as described would be highly effective. Unfortunately, the WorldCom infrastructure handling much of the data included an array of legacy systems with various underlying technologies.

In 1998, *NetworkWorldFusion* interviewed an advisory engineer working in the strategic accounts department at WorldCom’s primary network operations center in Richardson, Texas (Schultz and Watt 1998). The article reports staggering statistics related to the complexity of the WorldCom back-end systems: thousands of mainframes (Amdahl, Hitachi, and IBM) and minicomputers (Digital, Hewlett-Packard, Sun Microsystems, and from companies no longer in business) located in data centers across the country (Colorado Springs, Pentagon City, Cedar Rapids, etc.). With this network, WorldCom provided $1.6 billion in outsourcing services and managed more than 200 customer networks in addition to their own operations. The engineer joked about the Year 2000 problem, "We have so many systems, it would take us until 3000 to write custom applications for them." Figure 3 depicts the data flow of telephony traffic from origination (telephone switches) to legacy mainframe traffic and billing systems to ultimately the SAP consolidated financial reporting application.

The acquisition frenzy during the 1990s (more than 60 companies) created significant challenges for WorldCom management. Rather than requiring the acquired companies to migrate to WorldCom applications, management routinely elected to retain the acquired systems and create complex interfaces. KPMG identified over 30 billing and accounts receivable systems outside SAP during the restatement audit in 2003.[4] A CA Analyzer that only reviews data from the SAP general ledger and subledgers fails to consider the audit assertions of completeness and valuation.[5] A serious question arises: "Does the consolidating financial reporting application contain all the data and are the amounts correct?" The question cannot be answered unless the CA Analyzer receives information from all legacy applications. With the data, the CA Analyzer can confirm the successful transmission of the interfaces to SAP to address completeness, and perform analytics such as recalculating bad debt reserves to confirm proper valuation. Receiving that data may not be a realistic expectation.

The necessary monetary and human capital costs as well as the overall time required to establish links to each of the billing applications drastically increases the scope. Consider also that the billing and accounts receivable cycle represents only one of the many WorldCom business processes. The implementation of a comprehensive, fully integrated continuous assurance process at WorldCom may have been too cost-prohibitive and time-consuming simply because of the myriad of legacy systems providing data to the SAP general ledger.

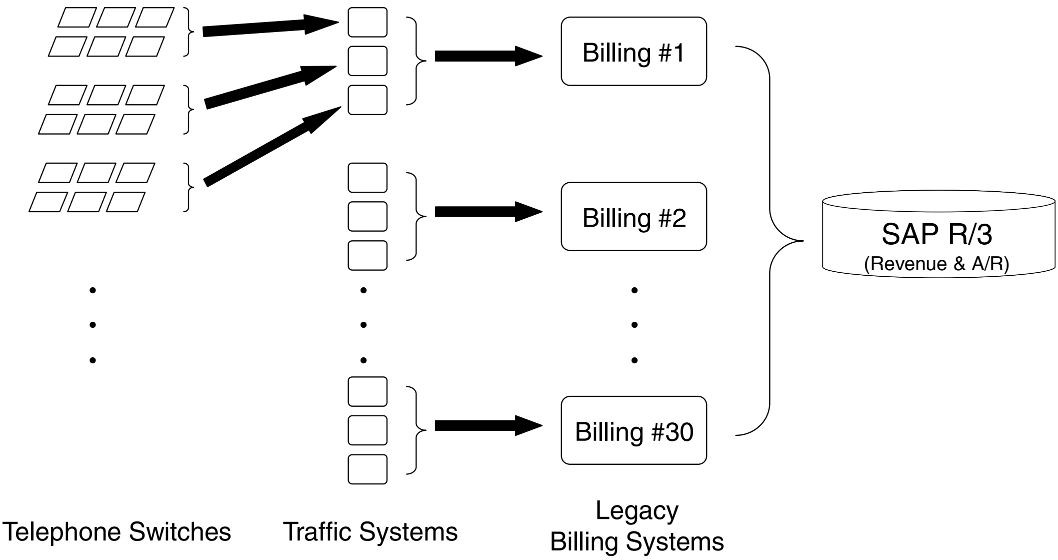
CONCLUSION AND IMPLICATIONS

The first few years of the 21st century have experienced significant change in the business environment due to unprecedented levels of corporate fraud. This paper examined the nature of the largest fraud in U.S. history and some of the techniques employed to manipulate financial information as a basis for considering how continuous assurance applied to substantive testing of accounts could facilitate early detection of fraudulent activity. WorldCom management categorized operating expenses as capital expenditures, reclassified the value of acquired MCI assets as goodwill, included future company expenses in the write-down of acquired assets, and manipulated bad debt reserve calculations. As illustrated,

[4] Regulators required MCI WorldCom to restate the financial statements from 1999–2002 to reflect accurate reporting (i.e., backing out of the fraud). KPMG performed the audit of the restated statements.

[5] Statement of Accounting Standard (SAS) No. 31 identifies the five general classes of assertions about which auditors are required to collect enough relevant information to lend credence to the items reflected in the financial statement: existence, completeness, valuation, rights and obligations, and presentation and disclosure. SAS No. 31 states "Assertions about completeness deal with whether all transactions and accounts that should be presented in the financial statements are so included." SAS No. 31 states "Assertions about valuation or allocation deal with whether asset, liability, revenue, and expense components have been included in the financial statements at appropriate amounts."

FIGURE 3
WorldCom Billing Process



monitoring analytics configured in a continuous assurance application operated and maintained remotely by the external audit firm provides a mechanism to detect irregularities comparable to those that occurred at WorldCom. The continuous assurance system facilitates this objective by extracting key financial data on a scheduled basis into a relational database and analyzing the information against a predefined rule-set (i.e., the MCL approach) that corresponds to traditional substantive-based tests of detail. Violations of the rule-set trigger automatic notifications to the auditor indicating further investigation may be required. Examining the WorldCom failure *ex post* obviously provides valuable insight in designing the analytics outlined in the study (i.e., hindsight is 20-20). However, the audit failure and fraudulent activity of a former Wall Street darling offers a rare opportunity to look back in order to move forward. The brief analysis of a few of the fraudulent activities and potential detection mechanisms lays the foundation for future research to develop a complete set of analytics beneficial to a broader domain.

The research also explored the implementation of continuous assurance procedures in an SAP-based environment based on the one utilized by WorldCom. The nature of ERP applications, SAP in particular, offers an environment conducive to continuous assurance. The SAP general ledger contains all accounting information for regulatory financial reporting in two tables, GLPCT and GLPCA. The continuous assurance application, as described herein, accesses the SAP instance via RFC to extract the table data directly from the SAP database into the auditor's continuous assurance system's relational database for analysis.

Complex computing infrastructures comprised of disparate applications and differing system platforms, however, complicate the implementation and ongoing use of a comprehensive, fully integrated continuous assurance system as a monitoring tool. As a case in point, this study presents the system environment at WorldCom that supported the traffic and billing processes. The complex network and interaction of legacy systems outside the SAP consolidated instance would have created a significant hindrance to the use of a complete continuous assurance system. As technology evolves to address current limitations and legacy systems expire, continuous assurance will continue to advance and offer even more viable opportunities than are currently available for increasing the audit quality and changing the overall attestation function.

Academic literature has focused primarily on progressing continuous assurance theory and, therefore, has been hindered by the lack of experimental and empirical research (Vasarhelyi et al. 2004). Recent research efforts (Alles et al. 2006) provide proofs of concept by designing and implementing continuous assurance applications into limited, controlled environments. To gain a better understanding of the overall feasibility and challenges to be faced, widespread implementation in complex system environments (i.e., legacy systems, ERP systems, e-commerce applications, etc.) must occur. In these implementation ventures, opportunities also exist for researchers to explore the integration of neural networks and other artificial intelligence techniques into the CA analyzer component at the heart of a continuous assurance system. The successes in earlier research that has used such techniques for fraud detection and bankruptcy detection offer great potential to enhancing the power and usefulness of continuous assurance applications. Research that integrates these concepts with continuous assurance models will make significant contributions.

Among the implementation challenges of any continuous assurance technology are certainly the initial cost of investment in terms of human capital and technological architecture, the ongoing consumption of system resources, the scalability of continuous assurance applications as technology changes, and the need to constantly refresh industry and economic trend data required for the accuracy and reliability of the underlying CA Analyzer rule-set. Academic researchers are well trained and prepared to research these types of constraints and barriers to continuous assurance, and should assume a leadership role in addressing these challenges.

Continuous assurance research should also begin to evolve beyond just the technical aspects of continuous assurance to also developing an understanding of the behavioral impacts of implementing such systems. From the auditor-auditee relationship aspect, there are a myriad of organizational and individual level effects that should be considered and addressed during the implementation of continuous assurance. For instance, how does continuous assurance affect the trust between auditors and auditees? Does continuous assurance encourage gaming behavior as auditees look to game the system when facing automated versus human auditing? From the auditor side of the relationship, there are also a number of concerns that have to be addressed. Automated continuous assurance does not eliminate the human component as interpretation of information still exists, but rather shifts the auditor's role to a certain degree as the auditor must learn how to sift through audit alerts, identify alerts that detect real problems, and determine appropriate follow-up procedures for unusual events detected on a continuous basis. Current prototypes have certainly provided evidence that there is typically a large volume of alerts generated, and the auditor must adjust. This suggests the relevance of applying existing theories of information processing in order to understand the impacts of information overload, information processing biases, and related information processing challenges that may uniquely exist in a continuous assurance environment. The opportunities for (and need for) research on continuous assurance hold great promise for researchers who wish to apply their research skills to moving practice forward and providing normative guidance on the basis by which continuous assurance should evolve and gain traction.

REFERENCES

Alles, M., G. Brennan, A. Kogan, and M. A. Vasarhelyi. 2006. Continuous monitoring of business process controls: A pilot implementation of a continuous auditing system at siemens. *International Journal of Accounting Information Systems* 7 (2): 137–161.

Alles, M., A. Kogan, and M. A. Vasarhelyi. 2004. Restoring auditor credibility: tertiary monitoring and logging of continuous assurance systems. *International Journal of Accounting Information Systems* 5 (2): 183–202.

———. 2002. Feasibility and economics of continuous assurance. *Auditing: A Journal of Practice & Theory* 21 (1): 125–138 (March).

American Institute of Certified Public Accountants (AICPA). 1980. Evidential Matter. Statement of Auditing Standards (SAS) No. 31 August. New York, NY: AICPA.

Bell, T. B., J. C. Bedard, K. M. Johnstone, and E. F. Smith. 2002. KRisk^{SM}: A computerized decision aid for client acceptance and continuous risk assessments. *Auditing: A Journal of Practice & Theory* 21 (2): 97–113.

Canadian Institute of Chartered Accountants and American Institute of Certified Public Accountants (CICA/AICPA). 1999. *Continuous Auditing*. Research report. Toronto, Canada: CICA.

Eichenwald, K. 2002. For WorldCom, acquisitions were behind its rise and fall. *The New York Times* (August 8).

Eining, M. M., J. K. Loebbecke, and J. J. Willingham. 1990. *Expert Systems: Issues for Decision Making in an Auditing Setting.* Proceedings of the Third International Symposium on Expert Systems in Business, Finance, and Accounting, Marina Del Ray, CA.

———, D. R. Jones, and J. K. Loebbecke. 1997. Reliance on decision aids: An examination of management fraud. *Auditing: A Journal of Practice & Theory* 16 (Fall): 1–19.

Feder, B. J., and S. Schiesel. 2002. WorldCom finds $3.3 billion more in irregularities. *The New York Times* (August 9).

Graham, L., and J. Bedard. 2003. Fraud risk and audit planning. *International Journal of Auditing* 7 (1): 55–70.

Groomer, S. M., and U. S. Murthy. 1989. Continuous auditing of database applications: An embedded audit module approach. *Journal of Information Systems* 3 (2): 53–69.

———, and ———. 2003. Monitoring high volume on-line transaction processing systems using a continuous sampling approach. *International Journal of Auditing* 7: 3–19.

Hackenbrack, K. 1993. The effects of experience with different sized clients on auditor evaluations of fraudulent financial reporting indicators. *Auditing: A Journal of Practice & Theory* 12 (Spring): 99–110.

Healy, P. 1985. Effect of bonus schemes on accounting decisions. *Journal of Accounting and Economics* (April): 85–107.

Kaplan, R., and D. Kiron. 2004. Accounting fraud at WorldCom. *Harvard Business School* (July 26).

Kogan, A., E. F. Sudit, and M. A. Vasarhelyi. 1999. Continuous online auditing: A program of research. *Journal of Information Systems* 13 (2): 87–103.

Pincus, K. V. 1989. The efficacy of red flags questionnaire for assessing the possibility of fraud. *Accounting, Organization, and Society* 14: 153–163.

Schultz, B., and P. Halper. 1998. Legacy lessons. *NetworkWorldFusion News* (October).

Sender, H. 2002. Accounting issues at WorldCom speak volumes about disclosures. *The Wall Street Journal* (August 21).

Vasarhelyi, M. A. 2005a. Would continuous audit have stopped the Enron mess? Working paper, Rutgers University.

———. 2005b. Concepts in continuous assurance. Working paper, Rutgers University.

———, M. Alles, and A. Kogan. 2004. Principles of analytic monitoring for continuous assurance. *Journal of Emerging Technologies in Accounting* 1: 1–21.

———, and F. B. Halper. 1991. The continuous audit of online systems. *Auditing: A Journal of Practice & Theory* 10 (1): 110–125.

Winograd, B. N., J. S. Gerson, and B. L. Berlin. 2000. Audit practices of PricewaterhouseCoopers. *Auditing: A Journal of Practice & Theory* 19 (2): 175–182.

Woodroof, J., and D. Searcy. 2001. Continuous audit: Model development and implementation within a debt covenant compliance domain. *International Journal of Accounting Information Systems* 2 (3): 169–191.