ELSEVIER

International Journal of Accounting Information Systems
5 (2004) 183–202

INTERNATIONAL JOURNAL OF
ACCOUNTING
INFORMATION
SYSTEMS

Restoring auditor credibility: tertiary monitoring and logging of continuous assurance systems

Michael G. Alles, Alexander Kogan*, Miklos A. Vasarhelyi

Rutgers Business School, 180 University Avenue, Newark, NJ 07102-1897, USA

Received 31 March 2003; received in revised form 30 November 2003; accepted 1 January 2004

Abstract

The continuing series of business scandals, from Enron to WorldCom, have undermined the credibility of auditing and auditors. In response, the SEC and the AICPA have advocated greater reliance on continuous assurance (CA), which utilizes on-line information technology to produce audit results simultaneously with, or a short period of time after, the occurrence of relevant events. In comparison with the traditional financial statements audit, CA aims to be timelier, more comprehensive, more accurate and more supportive of the management process. However, even if CA accomplishes that goal, will that be sufficient by itself to help restore investors' faith in auditing? We argue that while CA is certainly useful if the problem behind firm failure is lack of information and analysis, it is no more effective than standard auditing in a setting in which managers and auditors collude to deliberately mislead investors. Indeed, its reliance on automated analytics based on auditor- and manager-determined benchmarks makes CA especially vulnerable in the event of fraud. To overcome this potential weakness of future CA systems, we propose that they be augmented with a "black box (BB) log file" that is a read-only, third-party-controlled record of the actions of auditors, especially in regard to their interactions with management and choice of audit metric and models. Comprehensive and secure in a way that the current system of working papers is not, and accompanied by sophisticated search and analytic algorithms, the log files will serve as an "audit trail of an audit", thus enabling an efficient and effective tertiary assurance system. We also argue that the strongest incentive to adopt logging is the replacement of SAS No. 96 with a new standard specifying that the audit documentation contained in the BB log has to be comprehensive in the sense that the auditor can rely on no other evidence but the BB log to support the issued audit opinion, e.g., in the case of litigation. Such a new standard will essentially leave it to the audit firms and to market forces to determine the extent and scope of logging, while ensuring that the intent of

* Corresponding author. Tel.: +1-973-353-1064; fax: +1-973-353-1283.
E-mail address: kogan@andromeda.rutgers.edu (A. Kogan).

doi:10.1016/j.accinf.2004.01.010

logging—to enhance the credibility of the audit by ensuring that it is better backed up by audit documentation—will be fulfilled.

Keywords: Auditor credibility; Tertiary monitoring; Continuous assurance systems

1. Introduction

The degree to which assurance adds value to communications between an auditee and its audience is directly related to the credibility of the auditor. Whatever their real cause, the effect of the current series of corporate scandals, especially Enron and the subsequent collapse of Arthur Andersen, has been to undermine public confidence in the audit profession. As the recently passed Sarbanes–Oxley Act of 2002 recognizes, restoring auditor credibility is now a matter of priority given the importance of audited financial statements in facilitating capital market transactions.

The Sarbanes–Oxley Act of 2002 emphasizes the need for more frequent reporting and assurance as a way of restoring public faith in financial statements.[1] In addition, both the SEC and the AICPA have put forward continuous assurance (CA) as a vital component in the set of needed reforms.[2] In a congressional testimony on February 4, 2002, Harvey Pitt, then Chairman of the SEC, called for the use of more timely and comprehensive disclosures and assurance to increase market confidence in financial reports, auditors and the actions of managers. AICPA Chair James Castellano testified that:

> The transition to new reporting and auditing models is going to demand not only new audit approaches but personnel of the highest caliber. With this in mind, the profession has been working actively in the following areas: Continuous Auditing or continuous assurance involves reporting on short time frames and can pertain to either reporting on the effectiveness of a system producing data or more frequent reporting on the data itself. An AICPA task force has concluded that the enabling technologies, if not the tools, required to provide continuous assurance services, are, for the most part, currently available. Their actual implementation will evolve with progressive adoption of the concept and the emergence of appropriate specialized software tools.[3]

CA builds on the power of a firm's underlying enterprise resource planning (ERP) and other systems to produce audit results simultaneously with, or a short period of time after, the occurrence of relevant events.[4] In comparison with the traditional financial statements

[1] "Companies must disclose certain information on a current basis." (The Sarbanes–Oxley Act of 2002).
[2] http://www.sec.gov/news/testimony/020402tshlp.htm.
[3] http://energycommerce.house.gov/107/hearings/02142002Hearing490/Castellano804print.htm.
[4] CICA/AICPA (1999) and Kogan et al. (1999). Vasarhelyi et al. (2004) provides a detailed examination of the principles underlying the analytic monitoring capability of CA and how it builds on the automation and integration capabilities of the firm's ERP system.

audit, CA aims to be timelier, more comprehensive, more accurate and more supportive of the management process. While attaining that goal is still a work in progress, and the implementation of CA remains in its early phases, topical interest has clearly reached critical mass. Several years of academic research and conferences culminated in the simultaneous establishment of centers for continuous audit research in the United States and the European Union in September of 2002. Three papers in a special issue on CA in the March 2002 volume of *Auditing: A Journal of Practice and Theory*—Alles et al. (2002), Elliott (2002) and Rezaee et al. (2002)—focused on clarifying the distinction between CA and current audit practices and describing the potential for new assurance products.

It is one issue, however, to see CA as the inevitable evolution of audit techniques in response to the emergence of the digital economy, and quite another for it to serve as the mechanism for restoring auditor credibility. Does CA, as currently envisaged and by itself, have the power to restore public confidence in the value of an audit?

Our conclusion is that CA cannot bear that burden alone because the essential problem with the current audit system is the lack of effective tertiary monitoring—the audit of the audit.[5] For a large part, the credibility of the auditor has been based on the reputation of the major accounting firms that did most of the largest audits. With those reputations undermined with each new corporate scandal, it is evident that the societal needs for assurance are demanding that auditors be subject to the same or more stringent quality and effectiveness reviews as other participants in the financial sector. In other words, the major auditing firms are no longer to be given a unique exemption from having to prove that their reputations are warranted simply because of who they are. Moreover, the legal liability and regulatory incentives for auditors to do a good job also have evidently proven to be inadequate, placing even more emphasis on the need for the direct tertiary monitoring of the effectiveness of an audit.

The main form of tertiary monitoring, at present, besides the SEC, is the system of peer review, but that developed its own credibility problem, with many instances of undetected systemic audit problems and clean peer review opinions. For example, Deloitte and Touche gave Andersen an overall favorable review even after the Enron and other potential audit failures came to light. Moreover, in its defense, even the best run peer review would have a difficult time doing much, given that it is meant to cover all the audit engagements of a major firm over a three-year period.

Furthermore, we argue that this shortcoming in tertiary monitoring is an even greater concern in a future CA-enabled audit environment than it is today. While CA is potentially far more timely and comprehensive than a current audit is, it is also vulnerable to collusive fraud or auditor incompetence because of its almost exclusive reliance on automated procedures. Once default settings are established for the automated analytics, all transactions that meet those standards, whether those defaults are correctly set or not, would be accepted essentially without further review. This is a particular concern if there is collusive fraud between auditors and managers. The ability of interested parties to manipulate such defaults makes the CA system arguably less effective than a manual audit system, where

[5] We consider primary monitoring as being provided by the firm's own internal systems, with secondary monitoring supplied by the external auditors.

there is always the possibility that a future change in the audit firm might result in questions being raised about transactions that had been accepted without question in earlier audit engagements. Indeed, this is what happened at WorldCom and Adelphia Communications when these companies removed their business from the tarnished Andersen.

To overcome this potential weakness of future audit systems, we make the case that CA has to be expanded to allow for a secure and comprehensive third-party review of the audit—a way of allowing cost efficient and effective "guarding of the guards". What we focus on in this paper is how to bring this capability to CA, by taking advantage of its own unique capabilities of automation and integration of audit and business processes. We argue for the creation of a "black box (BB) log file" of the audit process to provide the "audit trail of the audit". The BB log will capture the critical decisions that directly affect the audit, such as the benchmarks for the automated analytic procedures. This log file will be secure, read-only and searchable by a tertiary reviewer, thus allowing the review to be conducted at a level of detail that is currently unattainable.

While unique in its application and intent, the BB log file is somewhat analogous both to the BB carried by commercial airliners and to the security camera in a retail store. A plane's BB cannot fly the plane or prevent crashes, but it can help to identify what went wrong. Similarly, while the log file cannot replicate the audit in every detail, it will help unravel the critical decisions that led to corporate and audit failure, and, unlike with an airplane's BB, the knowledge that there will be ex post transparency will have an ex ante deterrent effect. The security camera also has a deterrent effect, as indicated by the fact that it is possible to purchase fake, nonfunctional cameras, but it does not preclude all attempts at theft. By the same token, a log file will not end all instances of audit fraud or incompetence, but it will enhance the audit's credibility by making the actions of auditors easier to review.

The BB log file that we propose should not only contain the current set of working papers as a proper subset, but also should be comprehensive in a way that working papers are not. Working papers are meant to support the audit opinion, not to provide a complete record of the audit engagement as a way of facilitating an audit of the audit. Document retention policies, and the sheer volume of collected audit evidence, require periodic working paper "cleanups" that are not a facilitating factor for the ex post review of the audit work. Sarbanes–Oxley-related regulations increase the requirements of audit document retention but are not sufficient for rapid and thorough ex post audit review. In addition, because they are internal work products and not intended solely for external review, working papers lack the built-in read-only tampering safeguards of a log file. The need for a BB log file to replace and supplement the current working paper system was vividly demonstrated in a recent case in which PricewaterhouseCoopers agreed to pay a US$1-million fine to the SEC for improperly altering audit work papers, both for adding and deleting documents, after it learned of a lawsuit against a client, SmartTalk Tele-Services.[6]

We contend that the technologies that make CA possible allow for a true transformation of auditing, not just its automation, and, thereby, also meet the broader goals of the SEC

[6] "Accounting Firm Agrees to $1 Million Settlement", by Jonathan Glater, *New York Times* (May 23, 2003).

and the AICPA to make CA the means of restoring the credibility of the audit profession. In the next section, we provide some background on the concept of CA. In Section 3, we examine whether CA is indeed capable of preventing recurrences of the sorts of financial scandals that have undermined auditor credibility. Once we conclude that CA, as it now stands, cannot meet that burden, we turn in Section 4 to an examination of tertiary monitoring and how a log file is needed to make it more effective. Section 4 also provides a detailed analysis of both the content and the organization of a credible logging system. While we introduce the concept of the BB log file in this paper, we emphasize that there are many issues regarding its nature, technology, content and enforcement that the audit profession, interested constituencies and audit users must jointly reach consensus on. Those questions are examined in Section 5, where we propose the most important change to be made to ensure that the auditor will indeed create the BB log file as the true audit trail of the audit. Our proposal is to replace SAS No. 96 with a new standard specifying that the audit documentation contained in the BB log has to be comprehensive in the sense that the auditor can rely on no other evidence but the BB log to support the issued audit opinion, e.g., in the case of litigation. This proposal gives the audit firms and the market for auditing the freedom to determine the optimal scope and depth of auditing, while ensuring that the societal goal of more credible auditing through the development of a comprehensive system of auditing is brought to fruition. Section 6 discusses auditor rotation, which has been debated recently as a step towards restoring auditor credibility. We argue that rotation only strengthens the case for logging as a means of preserving the institutional memory of the audit, and this application further demonstrates the potential of the logging concept. Section 7 offers concluding comments.

2. The development of CA

In the period from 1986 to 1990, AT & T Bell Laboratories developed the continuous process auditing system (CPAS), as described in Vasarhelyi and Halper (1991). The system, designed for AT & T's corporate internal audit, created an overlay methodology to monitor the performance of one of the largest corporate customer account management systems that covered most of the customer relationship cycle. Vasarhelyi and Halper (1991) argued in that paper that this methodology had the potential to fundamentally change the timing, the nature of evidence and the process of auditing. In 1999, the AICPA and CICA published their joint study, further defining the field and laying out some alternative approaches (CICA/AICPA, 1999). It defines a continuous audit 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" (CICA/AICPA, 1999, pp. xiii). A program of research in CA was developed by Kogan et al. (1999). In 2000, the AICPA created the "Continuous SysTrust Committee" to evaluate the need for auditing standard changes for the advent of a more CA methodology.

The generic characteristics of a CA methodology will entail (1) a layer of software (aimed at process control and monitoring) on top of most critical corporate software systems, (2) an instantiation of the control and monitoring process aimed at business

process assurance by both internal and external assurors, (3) a constant stream of measurements (metrics) engineered out of key processes, (4) a sophisticated dynamic set of standards (models) to compare with the metrics, (5) a set of dynamic exception metrics to determine when an alarm is to be issued, and its degree of importance, (6) an analytic layer to perform additional analysis related to several corporate functions (auditing, fraud evaluation, accounting rule compliance, estimate review) and (7) a new level of statutory reporting that may include reports to governmental agencies and, potentially, BB logging.

The continuous audit methodology that we discuss in this paper is today the focus of intense interest by both accounting academics and practitioners and has been researched, developed and adopted, as least in part, by leading professional firms around the world. Our focus here is on its possible contribution towards restoring auditor credibility.

3. Tertiary monitoring and peer review

One explanation for the current wave of corporate scandals that has the smallest set of broader implications is that they are nothing more than examples of poor management and/or auditing (the ‘‘few rotten apples’’ theory). However, the hypothesis behind corporate failure that has gained the most currency in the public’s mind is that it is due to deliberate fraud between managers, aided and abetted by auditors, who, at best, are incompetent and, at worst, corrupt and outright compliant. To the extent that this is the perception of users of audit reports, whether their concerns are justified or not, they have to be addressed if auditor credibility is to be reestablished.

A situation in which company officers are carrying out deliberate fraud poses the greatest challenge to any audit system, and CA is no exception. Moreover, unlike in a case of poorly designed controls or a lack of clear communication, fraud, especially when aided and abetted by members of the audit team, raises the possibility of deliberate manipulation of the CA system itself. The strongest new capability that CA brings to control is the ability to continuously monitor and analyze large amounts of company data, enabling the implementation of an unprecedented set of analytic tests and real-time alarms. But the automation that underlines this capability can also be the basis for undermining the entire CA system if the managers being monitored, in collusion with audit team members, are able to influence the settings and parameters of those tests and alarms.

For example, if the CA is programmed to consider the formation of a special purpose entity (SPE) as a ‘‘routine transaction’’ that does not warrant any special attention, then such transactions would never trigger alarms in the CA system thereafter. Similarly, in WorldCom, the CFO might conceivably circumvent analytics designed to track unusual patterns in expenses and assets by suitably adjusting the alarms in the comparison metrics.

The potential for the CA system to be manipulated challenges the stated view of the SEC and the AICPA that CA is a part of the solution to the profession’s credibility problems. While CA has the potential to substantially improve the quality and reliability of the audit process, its ability to resist collusive fraud needs to be strengthened. In

particular, the processes for monitoring and controlling the audit itself have to be reexamined.

It has long been assumed that auditing is largely sufficient to serve as the secondary monitor on management, with bankers, analysts and credit agencies playing a backup role. But the recent malfeasance crisis was brought about by a systematic failure on the part of all the parties involved in corporate governance. The independence of external auditors, who are paid directly by the auditee and who have been obtaining an increasing amount of their revenue from consulting rather than auditing, has been brought into question. Analysts too have incentives not to confront management because of their links with investment bankers, while bankers already have been tarnished by the allegation that they issued IPOs at low prices and then allocated them to executives that would provide them with business. Auditors do face incentives to perform from the threat of legal liability and regulatory intervention, but these forces also have evidently proven to be insufficient to ensure credible auditing.

In short, we are back to the question of "who guards the guards?" In other words, what mechanisms are there to ensure that secondary monitoring is being carried out effectively? The lack of credible tertiary monitoring is a critical missing link in corporate governance, especially in the case of auditing. Tertiary monitoring of auditing currently consists of reviews of required filings and financial statements by the SEC and other entities, such as the FDIC of banks and the peer reviews of auditors. However, the adequacy of these practices has recently been brought into question. The SEC rarely conducts reviews of firms, partly by inclination, but mainly because of a severe lack of funds to hire staff accountants.[7] The fact that Andersen successfully passed a peer review during the Enron debacle has reduced investor confidence in that procedure.[8]

The ability of the current system of peer review to serve as an effective form of tertiary monitoring is constrained by the scope of the work involved. A peer review only takes place once every three years, during which time a major audit firm has completed several thousand engagements. An in-depth review of every audit is prohibitively costly and wasteful, even if it were feasible, given the amount of working papers and underlying audit data involved. But a superficial examination becomes a rubber stamp with little detection or deterrence value. In particular, colluding managers and auditors can evidently sidestep such a review and could perhaps do so even more easily when auditing is CA enabled.

The technological capability of CA, however, allows an endogenous solution to be developed for the shortcomings of its automated testing processes and default setting procedures. That automation can be transformed into strength by making use of it to create a new and more effective form of tertiary monitoring.

---

[7] A recent article in the *New York Times* [December 1, 2002, "In Stormy Time, SEC Is Facing Deeper Trouble"] states about the SEC that its "enforcement division and its office of compliance inspections, are understaffed by hundreds of officials, sharply limiting their effectiveness. Its corporate finance department cannot keep up with the deluge of company filings. Its market regulation division has for years been unable to persuade the agency's five commissioners to adopt rules of enormous consequence to the way the markets set stock prices." The 2003 federal budget, however, includes a large increase in funding for the SEC.

[8] http://peerreview.aicpaservices.org/firmfile/firmdetail.asp. Indeed, no major audit firm has ever received a negative peer review opinion, despite many well-publicized cases of audit failure.

4. Guarding the guards: tertiary monitoring using log files

4.1. Establishing an audit trail for the audit

Restoring auditor credibility, especially when auditing is CA enabled, requires a more effective form of tertiary monitoring. Keeping track of the defaults built into the CA system and clearly establishing lines of responsibility, the BB log file will serve as a permanent record of significant results and policy decisions in an audit and allow for third-party review.

Logging will bring to the audit environment, for the first time, an audit trail of the audit itself and the complementary data necessary to reconstruct key events. The aim of the BB log file is to allow a third-party reviewer to cost-effectively establish how the auditors did their job and, in particular, what role the client had in affecting the behavior of the audit team. By facilitating ex post review, logging will enhance the credibility of auditing by making the audit process more transparent. Such a system may not have stopped, e.g., Enron and Andersen from signing off on the SPEs the first time they arose, but at least, it would have made it clear to all participants that their "fingerprints" were on the relevant decisions. By eliminating deniability, the "taking the fifth" by the responsible parties would also be moot because objective records would exist of what they knew, when they knew it and what they decided to do.

Given the overriding objective of enhancing auditor credibility by facilitating tertiary monitoring, the BB log file will have to reflect a deep understanding of the desirable audit parameters and what types of major decisions affect its ultimate effectiveness. The logic behind the log file concept is that while audit standards and procedures lay out how an audit is broadly meant to be carried out, in practice, a series of decisions, some infrequent, some on a day-to-day basis, ultimately determines the thoroughness and effectiveness of the audit. In particular, in the case of CA, the tests and alarms built into the system and their default settings crucially affect the audit's capability and scope.

The BB log file that we propose goes well beyond the currently existing audit documentation requirements as implemented in the audit working papers. As was stated in the Introduction, the intent of the working papers is to support the issued audit opinion, which implies that they are periodically "cleaned up" to remove material superfluous to that purpose.[9] But as the recent case of PricewaterhouseCoopers, as well as the document handling problems at Andersen, indicate, intent can conflict with the broader openness needed to ensure auditor credibility in circumstances where the good faith of the auditor and the auditee are brought into question.

By contrast, the BB log file is a new tool expressly designed to enhance auditor credibility by taking advantage of the technological capabilities of the underlying CA

[9] On the other hand, audit working papers are sometimes data dumps, containing, e.g., bundles of trivial, irrelevant information. A predictable consequence of documentation retention policies, designed to shield firms from litigation rather than to facilitate peer review, has been to make firms simultaneously avoid discarding superfluous information while carefully massaging what relevant information is included. The eventual full migration to electronic working papers and the current litigious environment will accelerate the retention of extremely large amounts of data, albeit not necessarily in a form that will facilitate peer review.

system.[10] Critical for the effective working of the log file are its content, organization and security. While the working papers are intended only to support the audit opinion, the BB log file has to provide a comprehensive record of the entire audit process and the metainformation necessary to provide context to the log's content. To facilitate peer reviews, the BB log file has to be organized in such a way as to make possible automated information retrieval and search. And perhaps, most vital of all, the log file has to be secure against manipulation and data destruction, by being read-only and stored in a third-party repository.

4.2. Content of the BB log file

The purpose of the BB log is to provide an understandable audit trail of the audit, while the BB log must clearly identify the critical audit decisions that we call the audit's "inflection points", which by itself would not allow the recreation of the entire audit process. For the BB log to facilitate the restoration of auditor credibility, it should contain a substantive record of the most important automated and human activities related to the audit. This includes the detailed information provided by the client, such as various account balances and schedules, copies of contracts, the description and the results of the audit tests and procedures performed, such as analytical procedures, tests of detail, reprocessing of various calculations, the documentation of correspondence with the client, the confirmations obtained from third parties, and, most of all, the key discussions within the audit team and with the client on accounting treatment, estimates and adjustments.

Because in the current audit system, the evidence of the type described above is provided by the audit working papers, a BB log has to include the working papers as a proper subset. However, the wider scope envisioned of the BB log compared with manual working papers—facilitating tertiary monitoring of the audit process, not just supporting the audit opinion—suggests that while it is necessary to include the working papers in the log, even much more information will be required to record all the activities of the audit process. There is a far greater degree of discretion and individual judgment currently allowed in what goes into working papers than is desirable in a log file. One way of thinking about the difference between the two is the question of the burden of proof: Material is not included in the archived working papers if the case cannot be made that it is needed to support the audit opinion, while in the case of logging, an argument would have to be made for why material should not be included in the log file. Given the low cost of data storage and the sophistication of the search algorithms of the log file (to be discussed below), such an argument is meant to be difficult to sustain, except in rare circumstances.

The BB log will have to include a detailed time schedule of audit tasks performed by the engagement team and reviews performed by managers and partners. The log also needs to capture all changes over time to the electronic files and databases of the CA system. This will include not only various transactional and master data, but also relevant changes made to the settings of audit systems, with the latter done automatically through direct

[10] While some form of the log file system could, in theory, be implemented in a non-CA audit environment, in practice, it would be cost ineffective and technologically weaker, especially in terms of timeliness and security.

incorporation in the audit information systems. Automated logging components have to be implemented in CA and other audit automation systems to capture all newly created electronic documents as well as digitized paper documents related to the audit.[11]

However, not all information that is relevant to the log is in a form that is susceptible for automatic capture. Hence, the BB log also will have to be equipped with a special user interface to make it possible for properly authorized manual entry of certain information directly to the log. Obviously, this can be a potential weak spot in the logging process, and particular safeguards will be needed for manual entry. The BB log has to capture the attributes of every item, such as the identity of a person or process adding the information and the time of entry. All entries in the log must have unique identifiers that will be utilized for both indexing the log (to facilitate the search) and creating cross references between the log entries.

No entry to the log can be altered after being added. Even if an audit procedure is found to be deficient, its record still will remain in the log. This is essential for the log to serve as an audit trail of the audit. This feature of the log makes the proposed logging system substantively different from the current approach to audit working papers, which does not necessarily preserve identified deficiencies in the audit work, but only the final corrected results.[12] Even the enhanced audit documentation standards of the new SAS No. 96 on audit documentation, which require the identification in the working papers of all critical audit decisions (Whittington and Fischbach, 2002), are not sufficient to support effective tertiary monitoring because reasonable people can disagree about whether a certain decision is critical or not. This creates enough ambiguity to hinder the postmortem analysis of the audit process. Whatever is identified as important or critical ex ante may not correspond to what turns out to be important or critical ex post. SAS No. 96 continues to support the view expressed in SAS No. 41, that the audit documentation contained in the working papers does not have to be comprehensive, and other evidence can be relied on, e.g., in the case of litigation.

Only the creation of a true audit trail of the audit can support really effective forensic analysis of failed audits and therefore enable effective tertiary monitoring. At the same time, the presumption behind logging is that fewer audits will fail if all the parties involved are cognizant of the fact that a true audit trail of the audit is maintained. Thus, the true measure of the effectiveness of the BB log file, as with auditing itself, is its deterrent effect on both managers and auditors. Raising the deterrent effect of tertiary monitoring cascades down to the deterrent effect and, hence, to the credibility of secondary monitoring by the firm's external auditors.

4.3. Organization of the BB log file

The organizational structure (i.e., the format) of the BB log has to be designed to avoid the problem with manual working papers, that they do not facilitate review because of the

[11] The vast literature and practice on version control technology and software can help in reducing the bulk of storage and improve the ability to recreate audit situations at any time of the audit.

[12] The working papers standard—SAS No. 41, 1982—was recently replaced with the audit documentation standard—SAS No. 96, 2002 (see Whittington and Fischbach, 2002).

volume of data involved and the lack of a meaningful and comprehensive search facility. In particular, to enable effective tertiary monitoring, which still has to grapple with reviews of thousands of engagements over several years, the BB log has to be searchable by automated utilities that will be configurable and allow exception reporting to the reviewer. To be effectively searched, the BB log must record substantive amounts of relevant information in the first place, as discussed above. It is important to emphasize, however, that complete and relevant content is only necessary, but not sufficient, for enabling effective and efficient tertiary monitoring. The cost of information processing may turn out to be prohibitive, particularly in paper-based systems. It is crucially important to have a standard defining not only the content but also the format and organization of the logging mechanism.[13] The absence of such a standard may lead to the BB log file being reduced to a digital dumpsite, where truly useful information is buried in such a way that it is impossible to find. In other words, instead of encrypting relevant information, it can be hidden in plain sight by surrounding it with a mass of irrelevant data, thus avoiding the accusation of a cover-up.

This problem is not easy to overcome, and, in the extreme cases, such problems are indeed intractable, as shown by the successful use of the technique of steganography for cryptographic purposes (see, e.g., Stallings 1999). Although accounting and auditing standards setting history seems to suggest that developing a detailed log file standard will be nontrivial, certain logging guidelines are likely to be acceptable to most parties involved. The more detailed these guidelines become, the more useful the audit log file will be.

The organization of the log file is obviously a function of the type of information to be recorded. To be a useful tool for tertiary monitoring, the BB log file must clearly identify the inflection points of the audit—the critical decisions that determine its shape and scope—and differentiate them from the routine decisions that make up an audit. This information should already be preserved in the audit working papers (according to SAS No. 96), but not in a form that is straightforward for a tertiary reviewer to isolate and analyze.

One way of defining the organization of the BB log file is to begin with a template for a generic audit (albeit one differentiated by industry and auditee size) and then to clearly identify the decisions that move the audit away from this template. The aim of this tagging is to facilitate the tertiary monitoring of the points of departure of a particular from a generic audit, for that is the first priority for a peer review. Other aspects of the audit also have to be logged, but they would be tagged with a lower priority and turned to only if the exceptions file indicated that there was something that warranted a deeper examination.

Software packages for logging may come preloaded with the generic templates for an audit. Setting up the BB log file for the first time will be admittedly time consuming, assuming that a manual rather than an automated procedure is needed to list the specific changes needed to transform the generic to the specific audit, but that is a one-time task. The kind of inflection points that the BB log will tag include referrals from the audit team

[13] The purchase of third party logging software with unchangeable, preprogrammed routines, in addition to discretionarily definable logging features, may increase the robustness of the solution.

to the audit firm's accounting policy committees seeking guidance for specific applications of GAAP. While the auditor will have the ability to manually enter data, special automated procedures have to be developed to ensure that data is neither deliberately left out of the log or misfiled with the intention to mislead. These automated monitoring procedures can utilize artificial intelligence and natural language processing techniques to undertake the automatic categorization of filed items based on semantic matching of various terms to identify and properly tag important audit decisions.

While there are numerous technologies that can be utilized to implement logging, the best solutions will be identified only after extensive research and experimentation. While we call the log a "file", it will require extensive research and experimentation before a justifiable decision can be made about whether a system of flat files can be utilized to implement the BB log, or whether it actually has to be a database implemented in a major DBMS, like Oracle or DB2. The relational database technology is mature and well established and can therefore provide a stable technological foundation for the implementation of the BB log. One likely technological challenge will be due to the abundance in the log of binary large objects, such as lengthy Excel spreadsheets or document page images. Such binary objects will have to be included in the log for a number of reasons: (1) certain CA procedures will generate their results in such form, (2) certain external systems will provide documentary evidence in such form and (3) certain evidence, which is available on paper only, will be captured in such form. This will necessitate the development of special search procedures to allow for efficient access to various parts of the log. Another difficult issue associated with utilizing a relational database implementation of the BB log has to do with the associated reliance on a particular commercial database vendor (be it Oracle, IBM or Microsoft). The undesirable aspects of such reliance can outweigh the benefits provided by a relational database.

4.4. Integrity, security and confidentiality of the BB log file

The most essential prerequisites for the BB log's effectiveness and adoption are its integrity, security and confidentiality, for otherwise, it would lose its significance as a basis of tertiary monitoring. The BB log has to be private and secure in its contents and be inviolate to change, i.e., impossible to "shred". It has to be essentially read-only, with carefully designed tamper-proof procedures for the direct addition of information to the log by the auditors.

Both the regulation and implementation of the BB log will have to address the confidentiality concerns of all the parties involved. The BB log regulation will have to provide an explicit confidentiality policy specifying which parts of the log should be made available to whom and under what circumstances. The implementation of the BB log should provide access control procedures complying with the stated confidentiality policy. These access control procedures can utilize the role-based approach to deal with the complexity of the confidentiality policy.

The protection of the BB log against tampering can be based on implementing either preventive or detective controls. The standard tamper-proofing approach consists in writing the log to the write-once media, e.g., CD-Rs. Note that this may not be sufficient to preserve the log because the media can be physically destroyed. Therefore, the only

ultimate way to protect the log is to have it guarded by a custodian that will be both capable of and willing to prevent the log's destruction from happening, as well as have tools to detect omissions. The custodian of the BB log has to be an independent third party, such as the peer reviewer, the SEC, or a commercial firm, such as those that today guard offsite corporate computer backups. Another obvious candidate is the Public Company Accounting Oversight Board (PCAOB) created by the Sarbanes–Oxley Act of 2002.

One has to recognize that a transfer of the BB log to the custodian also creates significant challenges and problems. There will be organizational and technical problems related to the frequency and mode of the transfer, i.e., on-line versus off-line. Continuous on-line transfer of the BB log can become feasible only after a wide-scale comprehensive deployment of CA. Periodic on- or off-line transfer of the log seems to be feasible in the near future.

A major issue related to the transfer of the BB log to a custodian has to do with the expected concern on the part of the public accounting firms that other parties can have access to the log. While the Sarbanes–Oxley Act mandates the retention of audit working papers for the period of seven years, a subpoena is required to obtain these documents. It can be expected that public accounting firms and their clients will insist on an arrangement that will make it impossible for any other party to get access to the log without a subpoena and without the involvement of the firm.

A straightforward solution to this problem can involve the encryption of the BB log by the firm before the transfer to the custodian. While modern cryptographic technology is well developed and can be relied on to work as expected, this straightforward solution has an unexpected implication. If encryption is used, the preservation of the log file will not be guaranteed any more if the encryption key is kept by the public accounting firm only because with the destruction of the encryption key, the information content of the encrypted log cannot be recovered. An arrangement that will put the encryption key in the custody of yet another party may not be acceptable to the public accounting firms because the content of the log file can still be revealed if all the other parties collude. The solution involving the encryption key kept by the firm and log kept by the custodian provides superior assurance to the situation where the firm keeps the log because it prevents the firm from modifying the log after the fact.

It is possible to detect if the BB log has been tampered with after the fact without imposing the cost and complexity associated with the transfer of the whole log to the custodian. To achieve this assurance, we propose to use the technique of digital signatures (Stallings, 1999).[14] Instead of transferring the (unencrypted or encrypted)

[14] A digital signature is a message digest encoded using the private key of the signing party (in this case, the public accounting firm). The encoding is used to cryptographically authenticate the signing party. There are a number of different cryptographic algorithms that compute a message digest, including such popular ones as MD5 and SHA-1 (secure hash algorithm). Such algorithms transform an arbitrary length document D into a fixed-length document H(D). The length of H(D) is very short (only 128 bits in the case of MD5). These transformations have a number of important properties. First of all, miniscule changes to the document D will result in very significant changes to H(D). While H(D) is very easy to compute, there is no feasible computational procedure to compute D from H(D). Moreover, while the same digest is obtained from many different documents, none of these documents can be computed from the digest. It is also computationally intractable to create two different documents that have the same digest. This last property proves that the accounting firm cannot tamper with the log because it cannot create another log that has exactly the same digest.

BB log to the custodian, the firm will compute a digital signature of the log (or digital signatures of various parts of the log) and will transfer only this digital signature to the custodian. Because the digital signature is very short and easy to compute, the implementation of this transfer should be relatively cheap and simple. A digital signature by itself does not reveal any information about the content of the original log. If a BB log is subpoenaed later on, one can easily verify that the log corresponds to the digital signature kept by the custodian, and, therefore, this log has not been tampered with, although the verifier had absolutely no knowledge of the content of the log before it was subpoenaed. This last conclusion is based on the cryptographic properties of digital signatures and justifies the use of the term "BB" in the name of the log. The cost and complexity of this approach to assuring the integrity and security of the BB log are significantly lower as compared with the other approaches discussed above. However, the trade-off is the reliance on a detective control, which is not capable of preventing the destruction of the log.

It is possible to reduce the complexity of the problem of computing a digital signature of a huge BB log by decomposing the problem, i.e., computing digital signatures separately on parts of the log and submitting several of such digital signatures of the log parts to the custodian. It is important that this complexity and cost reduction can be achieved "for free" because the decomposition can be implemented without sacrificing any strength of the detective control. One can further reduce the cost and complexity by limiting the computation of digital signatures only to the most critical parts of the BB log and then transferring only these signatures to the custodian. It is doubtful that this further reduction can justify the associated inevitable weakening of the integrity and security guarantees of the BB log.

The above discussion demonstrates the trade-off between the strength of controls protecting the BB log against tampering and destruction and the level of privacy protection of the BB log owner, the audit firm. The strongest log protection provided by the transfer of the unencrypted BB log to a third-party custodian is associated with the highest exposure of the privacy of the log. The weakest protection provided by the transfer of the log digital signatures is associated with no exposure of the privacy of the log whatsoever. The other two approaches—transfer of the encrypted log to the custodian with the encryption key kept either by the log owner or by yet another third party—occupy the intermediate positions on the log tamper-proofing versus auditor's privacy continuum. The trade-off acceptable to all the interested parties will likely emerge only after lengthy deliberations.

5. Uses, enforcement and enablers of logging

5.1. Availability of the BB log file

When will the BB log file be made available for examination? Possibilities range from access granted only in the event of bankruptcy to review on a regular basis as part of the tertiary review process. Making the BB log file available only after a realized failure would provide the corporate equivalent of a flight data recorder, the BB that records the

instrument settings and cockpit voices of a crashed plane.[15] While having forensic and deterrent values, this approach does not substantially increase the real-time transparency of the audit process. A more aggressive alternative is to make the BB log or parts of it available for real-time review by the PCAOB or other overseeing agencies, which makes possible timely intervention by such an overseer in case of an ongoing critical audit failure. While the BB log file is primarily designed for use by the assuror of the quality of the audit work, be that a peer of the audit firm or another body chosen by the SEC or PCAOB, the BB log file's existence would also provide additional assurance for bankers, analysts, credit agencies, institutional investors and others concerned about the quality and integrity of the audited financial information provided by the company.

5.2. Enforcement of logging

How will logging be enforced? Logging itself is simply a tool that arises from taking advantage of the electronization of the firm and the ubiquity of ERP and, eventually, CA systems. Whether it can lead to the creation of a new and more credible system of tertiary monitoring is a function of whether auditors actually make entries into a BB log file. How is logging to be enforced? At one end of the spectrum, there is the possibility of official mandates from the SEC or PCAOB or from further congressional action. Generally accepted auditing standards (GAAS) will surely have something to say about the nature, composition and disposition of log files, in the same way as they provide guidance on working papers and other audit procedures.

As with CA (Alles et al., 2002), supply and demand within the marketplace may have a more immediate and long-lasting impact on the adoption of a tertiary monitoring mechanism, such as the log file. In particular, if logging increases the effectiveness of the assurance function and reduces the likelihood of fraud, then that will be reflected in a lower cost of capital and, perhaps even more importantly, lower insurance costs for the auditee, its officers and auditor.[16] This should prompt audit committees and audit firms themselves to require the use of logging and the specification of what should be logged.

One can argue that if a system like the BB log could indeed result from economic considerations, then we would already have large public accounting firms enhancing their audit working papers to the level of the BB log. Whether market mechanisms work to enforce audit logging, the enforcement of the BB log can surely be achieved through

[15] However, the level of complexity of the audit log BB is much greater. An airline flight recorder actually records in a continuous loop because the record of the last half hour or so immediately preceding the crash is all that concerns the investigators. In the case of corporations, failure might result from actions taken years before. But data storage is less of an issue, unlike in an airplane, where the size of the recorder is limited, and its design is dictated by the need to physically survive a crash. The flight recorder has a limited range of data that it tracks, while a far greater range of information will be needed in the case of a complex organization. Some conglomerates will presumably need a separate log for each organizational unit and audit arrangement. However, complex a BB log will be, it would still make a postbankruptcy investigation far easier, cheaper and faster than it is today, when it can drag on for years.

[16] The current spate of business and audit failures has resulted in a dramatic increase in liability insurance rates for directors and even the withdrawal of some coverage: "Insurance: Skyrocketing Rates, Plunging Coverage" *Business Week* (June 3, 2002).

standard setting and enforcement. The most important change that has to be made to ensure that the auditor will indeed create the BB log file as the true audit trail of the audit is to replace SAS No. 96 with a new standard specifying that the audit documentation contained in the BB log does have to be comprehensive in the sense that the auditor can rely on no other evidence but the BB log to support the issued audit opinion, e.g., in the case of litigation. We propose this change in the audit standard to create a crucial incentive for the auditors to create a comprehensive BB log because it is impossible to know ex ante what documentation the auditor will need ex post to defend the work performed on the engagement. Such a standard will make the evolution of logging subject to market forces, rather than relying on a standard setter to determine what is the optimal level of logging for all firms and in all circumstances. Thus, some audit firms may wish to electronically record (or videotape) all but the most trivial conversations between auditors and clients, while others may choose to rely on an ex post summary record placed in the log. The critical point is that the auditor has to stand or fall on what they chose to log at the time and cannot later claim to have based their actions on other communications with the client or on other discussions between the auditors.

Ultimately, no one can guarantee that individual auditors will actually file entries into a log file, but once logging is established in the corporate mainstream, the failure to do so would become both more visible and an a priori argument for misbehavior.[17] The enhanced liability protection that logging should provide the audit firm (especially when the local audit partners choose to ignore firm rules and not log) might induce the major audit firms to institute a system of BB logging in the first place. On the other hand, a real concern is that the existence of a BB log might induce secondary behavioral effects, including auditors not raising some key issues of accounting treatment precisely to avoid being logged. The institutional infrastructure of logging and its implementation is a subject that requires further and wider debate by the audit community.

5.3. CA as the enabler of BB logging

The scale and scope of information that will be logged in a BB log file is likely to be considerable. Without a CA system deployed, it is difficult to create an audit log file as described above. On the other hand, if a CA system is available, then, the requirement of maintaining the audit log file should not be too burdensome, partly because much of this data has already been collected by the enterprise information system for internal decision-making purposes and partly because it is not difficult to make the CA system log its formal activities. All that is happening is that the information is being stored in a secure and confidential way so that a third party reviewer can quickly find out and assess what managers and auditors are doing.[18] More fundamentally, though, the BB log file uses the unique technological capabilities of CA to develop new audit methodologies that are not

[17] For example, if Arthur Andersen had in place rules regarding what information the Enron audit team had to log about their treatment of SPEs, then it would have been much easier for the SEC to have apportioned blame for the audit failure between Duncan, attorneys and other members of the Enron engagement team and the company as a whole.

[18] A public/private key schema with the courts (or SEC) keeping the key could be adapted for this purpose.

currently feasible, as opposed to seeing CA as just an evolutionary technology for existing audit methods. It is the difference in perspective between reengineering and automation, and as business has found out, rethinking processes rather than rethinking technologies is the only way to access the productivity improvements that new technologies offer.

The implementation of BB log will pose many technological, organizational and regulatory and legal challenges. The regulatory and legal considerations will be of primary importance in determining the content and mode of logging. For logs to become a reality, public accounting firms will have to implement organizational process changes to facilitate logging. Such organizational changes will affect numerous matters ranging from correspondence handling rules to personnel decision-making procedures. The objective of these changes will be to institutionalize the procedures for the automated, semiautomated or human-facilitated digital capture of information required in the BB log. Because of the complexity of the issues involved, firms may have to be left to make specific decisions about how to implement the BB log, and to the enforcement body and/or (possibly) the legal system to ensure compliance of each particular implementation of the BB log with the regulation.

While the reliance on CA as the enabler can make BB logging feasible, the implementation of logging as described above will require significant investment of financial and human resources. Therefore, it is appropriate to ask who will be paying for BB logging. While market forces will determine the ultimate answer to this question, the additional cost of BB logging is likely to be eventually passed on to the payer for the audit engagement. But even if BB logging makes the statutory audit more costly, this societal cost will have to be balanced against the benefits that the implementation of BB logging will bring in restoring the credibility of auditors.

6. Logging to preserve institutional memory in auditor rotation or change

A great deal of interest has been expressed lately in the contentious idea of term limits for audit engagements, with mandated rotations of the auditor after three to five years.[19] While the recently passed Sarbanes–Oxley Act decided to rotate only the audit partner and not the auditor, the issue is far from settled. We discuss this issue here to further illustrate the potential and power of the BB log file. Utilizing logging to mitigate difficult problems and reduce costs associated with rotating auditors can be viewed as an extension and generalization of the following point of view expressed by the The Conference Board Commission on Public Trust and Private Enterprise (2003, p.34):

> The Commission recognizes that there could be some incremental costs to public companies in changing auditors on a periodic basis because the new audit firm would have to learn about the company's finances and operations. However, this transition could be facilitated by requesting, or requiring by contract, the outgoing audit firm to retain and transfer all its working papers to the incoming audit firm. The Commission

[19] Goldin H. Auditor term limits. *The New York Times,* February 1, 2002.

believes the cost of implementing this best practice may be significantly less than costs endured by investors in capital markets resulting from the loss of investor confidence in response to inaccurate financial statements.

The aim of mandatory rotation is to prevent a too close relationship developing between auditor and auditee, as well as to deter collusion because of the knowledge that a new auditor will scrutinize any prior arrangements and procedures. The audit profession has long opposed mandatory rotation, arguing that a long engagement allows auditors to gain experience and knowledge about the firm, as well as lowering overall costs for auditors, auditees and society in general (see e.g., Bell et al., 1997). It also has been argued that given the high startup cost of a new audit engagement, the new auditor will be especially reluctant to take on a new audit client to avoid jeopardizing the future rents necessary to recover the high sunk cost of the new engagement. Empirical research in auditing seems to support this point of view (Geiger and Raghunandan, 2002).

Whatever the merits and prospects of this proposal, it is useful to discuss the implications of a greater reliance on CA if term-limited audits come into practice. Alles et al. (2002) point out that CA will require a high setup cost as customized software is piggybacked onto the firm's ERP system because it would be impractical for the auditor not to take advantage of the firm's own IT architecture. They go on to discuss the critical question of who will own the CA overlay and the effect that different ownership and payment arrangements will have on auditor independence and the relative bargaining power of the auditor and the auditee. These questions are particularly relevant if the auditor has to be rotated every few years.

Unless an inexpensive standardized CA overlay system can be developed, as opposed to the highly customized systems in use today, presumably, the existing CA system will be transferred to the new auditor, and it is a good question whether that auditor has to bear any of the setup costs of this system. Most likely, the CA system will be based on the same monitoring and control platform as many corporate processes. Therefore, the cost of its installation is more of analytic setup and process understanding than the software itself. Much of this infrastructure may be transferable from auditor to auditor, regardless of this being auditor rotation or just auditor change. The benefits of CA in this term limited environment stem from the fact that having a CA system already in place would reduce the deleterious effect on audit efficacy of changing auditors. The CA system can keep monitoring despite the change in the auditor and deter management manipulation designed to take advantage of the transition period between auditors. A break in the continuum of auditing is much more likely in a manual audit setting, where much of the institutional memory of the audit—and its deterrent effect—would walk out of the firm along with the auditor.

On the other hand, the reliance of the new audit firm on a CA system, that it had no role in creating, is somewhat problematic. The ability of management to affect system settings and set defaults means that the new auditor will have to first audit the CA system, a task made difficult by its lack of first hand knowledge of how the system evolved. Obviously, the new auditor cannot overly rely on those who do have that prior knowledge of the CA system—management and the previous auditor—because that would undermine the logic of mandatory auditor changes in the first place. This difficulty with the transition between

auditors can be greatly ameliorated, however, if there is in place a BB log. The log will provide an objective explanation to the new auditor of how the CA system has reached its current state and the interactions between management and the previous auditor that gave rise to it. Furthermore, audit logs can be built as knowledge structures that explain what assurance procedures are automatically performed and how they interact.

The rationale for auditor rotation is a lack of trust that the auditor would not collude with management given the chance to develop a long-term relationship. Because that also is the basis of the setting that prompted the proposal for a BB log file, it is only to be expected that logging would be invaluable in a term-limited audit environment. It will serve as a source of impartial institutional and audit process memory that can survive auditor changes and also allow the new auditor to more quickly ascertain what kinds of changes the old audit team had made to the CA system and what defaults they had agreed upon. This latter task becomes feasible if meaningful guidelines related to the format and content of the log file are generally accepted.

7. Conclusion

The current spate of corporate failures and the collapse of Arthur Andersen pose the greatest challenge to the financial markets, public accounting and auditing since the Great Depression. This massive loss of public confidence places great pressure on the profession to undertake structural reforms rather than resorting to partial solutions. This opportunity to bring about much needed changes that would have never been seriously considered before is the saving grace of this episode that has seen the credibility of the audit profession severely undermined.

CA has been the source of considerable interest in the academic and professional communities over the last few years, but its utilization has yet to reach critical mass. But now, CA is increasingly been seen as potentially an important tool for auditors as they confront business relationships and practices far more complex than they were used to dealing with in the past. Nonetheless, it is important that the strengths and weaknesses of CA be fully understood. In particular, while the unique technical capabilities of CA enhance its inherent credibility and effectiveness over standard auditing, in the absence of an effective and credible system of tertiary monitoring, it is equally vulnerable in its reliance on the behavior and judgment of its users and reviewers. The proposed BB log file covers a fundamental weak point of the CA system, that the very people that it is meant to monitor can manipulate it. But the BB log is not meant to and cannot work alone. As much care must be taken in designing the institutional structure within which it operates—who examines CA data, who designs the base models to give benchmarks for data content and the scope and depth of the assurance.

References

Alles M, Kogan A, Vasarhelyi MA. Feasibility and economics of continuous assurance. Auditing: A Journal of Practice and Theory 2002;21(1):125–38 [March].

Bell TB, Marrs FO, Solomon I, Thomas H. Auditing organizations through a strategic-systems lens: the KPMG business measurement process. Montvale (NJ): KPMG Peat Marwick, LLP; 1997.

CICA/AICPA. Continuous auditing. Research Report, Toronto, Canada: The Canadian Institute of Chartered Accountants; 1999.

Elliot RK. Twenty-first century assurance. Auditing: A Journal of Practice and Theory. 2002;21(1):139–146 [March].

The Conference Board Commission on Public Trust and Private Enterprise. Findings and Recommendations, Part 3: Audit and Accounting, January 9; 2003. <http://www.conference-board.org/knowledge/governCommission.cfm>.

Geiger MA, Raghunandan K. Auditor tenure and audit reporting failures. Auditing: A Journal of Practice and Theory 2002;21(1):67–78 [March].

Kogan A, Sudit EF, Vasarhelyi MA. Continuous online auditing: a program of research. Journal of Information Systems 1999;13(2):87–103 [Fall].

Rezaee A, Sharbatoghlie A, Elam R, McMickle PL. Continuous auditing: Building automated auditing capability. Auditing: A Journal of Practice and Theory 2002;21(1):147–163 [March].

Stallings W. Cryptography and network security: principles and practice. Upper Saddle River (NJ): Prentice Hall; 1999.

Vasarhelyi MA, Halper FB. The continuous audit of online systems. Auditing: A Journal of Practice and Theory 1991;10(1):110–25.

Vasarhelyi MA, Alles MG, Kogan A. Principles of analytic monitoring for continuous assurance. Journal of Emerging Technologies in Accounting 2004;1:1–21.

Whittington R, Fischbach G. The new audit documentation requirements. Journal of Accountancy 2002;4(193) [April, http://www.aicpa.org/pubs/jofa/apr2002/whitting.htm].