BLACK BOX LOGGING AND TERTIARY MONITORING OF CONTINUOUS ASSURANCE SYSTEMS

By Michael Alles, Alexander Kogan and Miklos Vasarhelyi, Rutgers Business School

Introduction

In response to the unprecedented crisis of confidence in accounting prompted by the scandals at Enron/Andersen, Global Crossing, WorldCom, Adelphia and others, both the SEC and the AICPA have publicly endorsed **Continuous Assurance** in Congressional testimony. Continuous assurance (CA) is technology-enabled auditing which produces audit results simultaneously with, or a short period of time after, the occurrence of relevant events. Utilizing the power of online IT systems, CA provides the potential for a wider set of assurance reports encompassing a broader set of variables, alarms and analytic procedures. In comparison with a traditional financial statements audit, CA is timelier, more comprehensive, more accurate and more supportive of the management process.

But would continuous assurance be effective in preventing reoccurrences of the kind of corporate failures characterized by management fraud combined with inadequate auditing that have so shaken market confidence? In fact, CA may also be vulnerable compared to standard auditing,

given its reliance on default settings established by possibly collusive auditors and managers.

To overcome this "Achilles' Heel" of CA requires plugging a large hole in today's audit environment: the lack of an effective system of **tertiary monitoring**—the audit of the audit. This requires the development of a new system of logging, analogous to an airplane's "Black Box", that will enhance the effectiveness of the currently flawed peer review process and so help restore auditor credibility.

Corporate and Audit Failure

The explanation for the current crop of corporate failures 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 compliant auditors. For example, the treatment of $7.1 billion of expenses at WorldCom as assets is the most basic form of accounting fraud, and its auditor (Andersen, of course…) was harshly questioned in Congress as to the purpose of an audit if it could not capture such egregious earnings management. In other cases, such as Adelphia and Enron, managers flagrantly used

the firm's resources as their own, apparently without setting off any alarms.

A situation in which company officers are carrying out deliberate fraud, let alone one in which auditors are looking the other way, presents the greatest challenge to CA. Unlike in a case of poorly designed controls or management incompetence, fraud raises the possibility of deliberate manipulation of the CA system itself. The ability of CA to benchmark in real time data content against expected values and continuous relationship among processes, which is the strongest new capability it brings to control, can be made redundant if it is the parties being monitored who determine the transactions which trigger alarms. Thus, in the case of GlobalCrossing, if auditors and managers program the CA to consider a round trip as a routine transaction then *all* round trips would slip under the CA systems controls. The ability to set such defaults makes the CA system arguably less effective than a manual audit system, where there is always the possibility that an untainted new auditor might raise questions about previously allowed transactions—indeed, this is precisely what happened at WorldCom and Adelphia Communications.

It had long been assumed that the presence of an external auditor, especially one of the majors, was largely sufficient to deter management misconduct, with bankers, analysts and credit agencies playing a backup role. But the recent sequence of spectacular failures was brought about by a systematic failure on the part of almost all the parties involved in corporate governance, notably auditors safeguarding their consulting practices. Hence, the question that has to be now asked is "**who guards the guards?**"

While, that logic can be repeated ad infinitum, the presence of at least one other independent player besides the firm and a possibly compromised auditor is coming to be seen as a critical missing link in corporate governance. In fact, such third party monitoring of the firm and the auditor does exist now, through SEC reviews of financial statements and peer review of auditors. However, in practice, both these practices have proved to be inadequate to the task. The fact that Andersen successfully passed a peer review during the Enron debacle has hardly inspired confidence in that procedure.

Tertiary Monitoring and Black Box Logging

To increase the effectiveness—both real and perceived—of CA-enabled auditing we put forward the concept of the "**Black Box audit Log File**" (BB Log). Our proposal deters manipulations of the CA system by the auditor or the auditee by making such manipulation more visible, through the creation of a confidential "log" of audit

procedures (and other economic events) in the CA system. This CA logging proposal can be viewed as an extension of the existing practice of documenting audit activities in manual or automated work papers. The log proposal, however, goes far beyond the existing practice, by utilizing CA to systematically implement in auditing such standard control principles as adequate records maintenance, separation of duties and proper authorization of audit activities. The benefits of the log proposal also extend further than enhancing the integrity of the CA system—it can also be the foundation for a much more thorough and visible system of corporate governance by making feasible for the first time in our current audit setting of effective and credible tertiary monitoring.

A BB-log with sophisticated search functions would allow the tertiary monitor to extend a peer review down to the substantive procedures level of an audit, rather than being forced by the amount of data involved to be restricted to a test of controls only. The latter has clearly proved insufficient to catch or deter inadequate auditing or collusion with management.

The essence of the BB-Log is the creation of a permanent record of the most important audit procedures with an "audit trail" of its own. This log system should keep track of the defaults built into the CA system

and clearly establish lines of responsibility. It can serve as a gatekeeper between managers and significant policy decisions on an audit, requiring auditors and auditees to state what they are doing in a medium that will permanently record their actions and allow for third party review of them. Such a system may not have stopped, for example, 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 it. By eliminating deniability, the "taking the fifth" by the responsible parties would also be moot, since objective records would exist of what they knew, when they knew it and what they chose to do.

The key to making this system work is making the log itself selective, private and secure in its contents and inviolate to change, i.e., making sure that it is impossible to "shred". A variety of technologies and procedures have to be involved here. While access has to be granted to view the log, it would be "read-only" and encrypted. The master records may be kept under the supervision of a 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

created under the recently passed Sarbanes-Oxley Act.

Figure 1 describes a summary view of the proposed BB Log, which includes three complementary log streams, a log of key transactions and events, a log of selective control actions and processes and a log of audit processes drawn from actions in automated working papers. These logs, together, allow for the re-creation of the economic circumstances at the auditee, in a certain moment in time, and the evaluation of the auditor's actions. A more severe form of BB logging would add filters and sensors to the configuration adding information to the monitoring process, capturing XML-based transaction data, examining the patterns of this XML data stream, applying AI pattern recognition techniques to identify ongoing fraudulent patterns.

Insert Figure 1 here

Implementing and Using BB-Logs

This is only a preliminary proposal and many issues need to be discussed about how the log system will work in practice. How these questions are answered will greatly affect the power and scope of the log file system and determine whether logging becomes just a supplementary tool of the existing audit and peer review process, or

whether it can help create a thorough system of tertiary monitoring:

- **When will the audit log file be made available for examination?** Possibilities range from access granted only in the event of bankruptcy, to regular analysis by a tertiary monitor as part of the peer review process. Making the log files available only after a realized failure would provide the corporate equivalent of a flight data recorder, the "black box" that records instrument settings and cockpit voices, so facilitating failure analysis.

- **What information will be tracked?** The BB Log proposal could be implemented at several levels of complexity or intrusiveness. The extremes would be pure archival (data is gathered and dropped in an external trusted bucket) to dynamic interactive use where extensive analytics are performed in the data streams, alarms generated, summarization and synchronization performed, statutory reports generated, and notes to archive examiners introduced. At this level a BB-Log becomes a proactive tool that extends CA scrutiny, acts as an intrusive deterrent of management and auditor malfeasance, and may feed third party continuous supervisory algorithms. Eventually, very advanced forms of intrusion could be designed with process interruption

routines or activation routines that bring in additional processes from the organization or trusted parties. Figure 2 illustrates how basic and extended logging might have been implemented, and some basic functionalities, in some of the firms involved in the current set of scandals.

Insert Figure 2 here

- **Amount of storage required, confidentiality and materiality**: The economics of data storage would impose a technical limit on the scope of the log file. Furthermore , in practice, issues of confidentiality, security, intrusiveness, and materiality have to play a role. Care has to be taken to prevent the audit log file from being reduced to a digital dumpsite where truly useful information is buried in such a way that it is impossible to find. The BB log, if implemented, would force organizations to have rehearsals of the use of the data together with catastrophe planning. Additionally, a well planned log could be used as an extreme form of data backup or as a methodology to satisfy statutory data retention requirements.

- **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 from further congressional action. Generally accepted auditing standards (GAAS) will surely have something say about the nature, composition and disposition of log files, in the same way as they provide guidance on analytic tests. But supply and demand within the marketplace is likely to have a more immediate and long-lasting impact on the adoption of a tertiary monitoring mechanism such as the BB Log File. In particular, if logging increases the effectiveness of auditing 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 firm, its officers and auditor. This should prompt boards of directors and audit practice oversight committees to require the use of logging and the specification of what should be logged.

Conclusion

The scale and scope of information that will be logged in a log file is likely to be considerable. It is quite clear that 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 because much of this data would already have been collected by the ERP system for internal decision making purposes, and also because it is not difficult to implement logging in a CA system. What is critical in BB-logging is that the information is being stored in a secure and confidential way so that a tertiary monitor can quickly and cost-effectively find out and assess what managers and auditors are doing.

More fundamentally though, the log file is making use of the unique technological capabilities of CA to develop new audit tools that were not feasible before, 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.
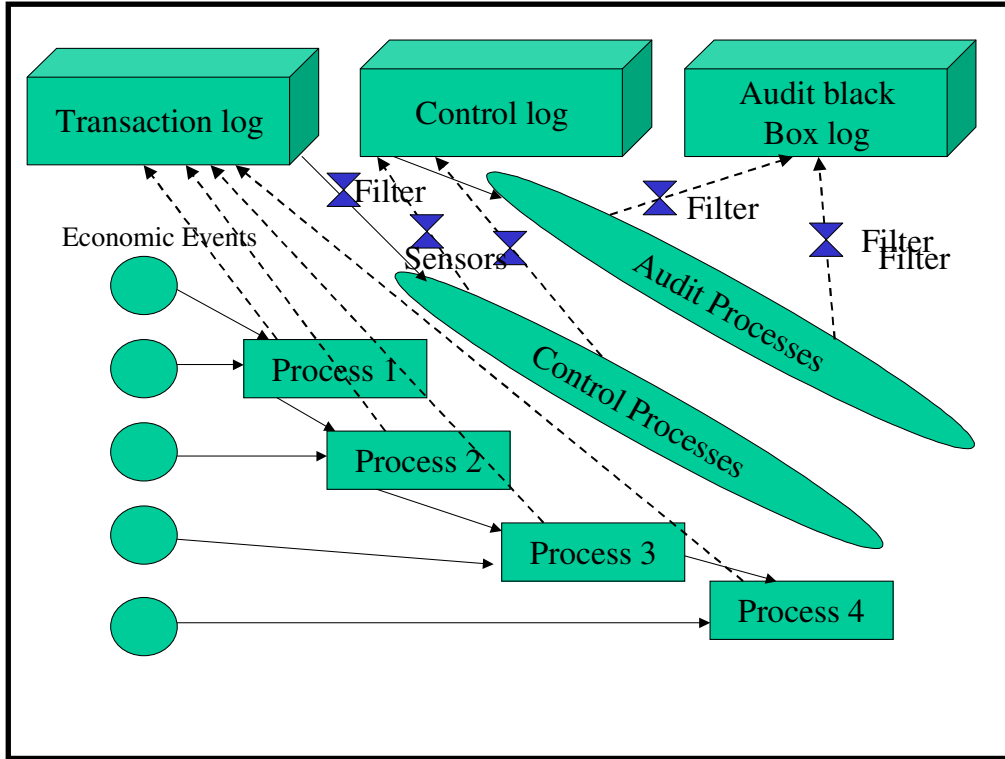
Figure 1: Levels of Logging

Sensor

Figure 2: Comparison of CA to basic and extended BB-Logging

Company	Problem	Continuous Assurance Potential	Basic BB-Log	Extended BB-Logging
ENRON	SPEs	Most likely the moves of Liabilities to SPEs would be flagged and require director's endorsements	Record of auditor awareness of SPE	Flags issued on awareness, notes by auditors, etc…
ENRON	Trading by executives	More difficult to detect particularly if on the name of family and associates, a third party trading monitoring system should be established by the stock-exchanges for monitoring	Records of treasury stock and options issued to executives and approvals by controls including compensation committee	Analytics relative red flags in these operations
Adelphia Communications	Loan guarantees to directors	Difficult to detect if an executive signs for the company without informing directors	Records if loans were approved and recorded—with proper controls their absence implies rogue guarantees/loans	Proactive system of contacts with banks and loan portfolio review
Quest	Round-tripping	Specific transaction logging and algorithmic matching would have easily identified even modified amounts and date lapping	Log of the transactions, the controls on the transactions and auditor acknowledgement (or ignorance) of these transactions	Red flags of matching transactions, pink flags of potential round-trip transactions.
WorldCom	Capitalization of operating charges	Vendor maps and summarization with continuity equations would have pointed out the problem, changes on rules of internal control are needed for transaction reclassification	Log of transactions and of flags generated by the CA system	Analytic maps of inconsistencies of accounting treatment within categories and required acknowledge by internal and external auditors
Halliburton	Adopting more aggressive policies last year about recording sales and postponing potential losses	Continuous monitoring of ratios would show dramatic change, internal control rules should require this being pointed to audit committee as a level 4 alarm	Records of income recognition and expenses	Identification of policy changes and their representation by responsible managers