THE CONTINUOUS AUDIT OF ONLINE SYSTEMS

Miklos A. Vasarhelyi
AT&T Bell Laboratories, 600 Mountain Ave., Murray Hill, N.J. 07974 and Rutgers University, Newark, N.J.
Fern B. Halper

AT&T Bell Laboratories, 600 Mountain Ave., Murray Hill, N.J. 07974.

Submitted to Auditing: A Journal of Practice and Theory
August 1989
Revised June 1990

The authors wish to thank the two anonymous reviewers for their constructive comments and the editor for his review of the manuscript. We would also like to thank the participants of research seminars at Columbia University, Rutgers University, the University of Kansas, the University of Nebraska, and Boston University and the attendees of the EDPAA, IIA, and AICPA professional meetings for their comments and suggestions. We are particularly indebted to Sam Parker, Chris Calabrese, Tsyh-Wen Pao, John Snively, Andrew Sherman, and Kazuo Ezawa for their work on the prototype system.

ABSTRACT

The evolution of MIS technology has affected traditional auditing and created a new set of audit issues. This paper focuses on the Continuous Process Auditing System (CPAS) developed at AT&T Bell Laboratories for the Internal Audit organization. The system is an implementation of a Continuous Process Audit Methodology (CPAM) and is designed to deal with the problems of auditing large paperless database systems. The paper discusses why the methodology is important and contrasts it with the traditional audit model. An implementation of the continuous process audit methodologyis discussed. CPAS is designed to measure and monitor large systems, drawing key metrics and analytics into a workstation environment. The data are displayed in an interactive mode, providing auditors with a work platform to examine extracted data and prepare auditing reports. CPAS monitors key operational analytics, compares these with standards, and calls the auditor's attention to any problems. Ultimately, this technology will utilize system probes that will monitor the auditee system and intervene when needed.

INTRODUCTION

This paper develops the concept and explores key issues in an alternate audit approach called the Continuous Process Audit Methodology (CPAM). The paper focuses on an implementation of this methodology, the Continuous Process Audit System, developed at AT&T Bell Laboratories for the AT&T Internal Audit Organization.

The paper is divided into four sections. In the remainder of the Introduction, changes in Management Information Systems (MIS) that affect traditional auditing are discussed. In the second section, CPAM and CPAS are described and contrasted with the traditional audit approach. The audit implications related to the introduction of a CPAS like technology also are examined. The last section discusses some of the knowledge issues involved in the implementation of a CPAS application and suggests paths for future work.

Technology and the Auditor

Traditional auditing (both internal and external) has changed considerably in recent years, primarily as a result of changes in the data processing environment. [Roussey, 1986 ; Elliot, 1986; Vasarhelyi and Lin, 1988; Bailey et al., 1989]. These changes have created major challenges in performing the auditing and attestation function. These changes and the technical obstacles created for auditors as a result of these changes are summarized in Table 1.

TABLE 1

The Evolution of Auditing from a Data Processing Perspective

Phase	Period	Data Processing of Functions	Applications	Audit Problem
1	1945-55	Input (I) Output (O) Processing (P)	Scientific & Military applications	Data transcription Repetitive processing
2	1955-65	I, O, P Storage (S)	Magnetic tapes Natural applications	Data not visually readable Data that may be changed without traces
3	1965-75	I, O, P, S Communication (C)	Time-sharing systems Disk storage Expanded Operations support	Access to data without physical access
4	1975-85	I, O, P, S, C Databases (D)	Integrated databases Decision Support Systems (decision aides) Across-area applications	Different physical and logical data layouts New complexity layer (DBMS)

				Decisions impounded into software
5	1986-91	I, O, P, S, C, D Workstations (W)	Networks Decision support systems (non-expert) Mass optical storage	Data distributed among sites Large quantities of data Distributed processing entities Paperless data sources Interconnected systems
6	1991-on	I, O, P, S, C, D, W Decisions (De)	Decision support systems (expert)	Stochastic decisions impounded into MIS

For example, the introduction of technology precluded auditors from directly reading data from its source (magnetic tape) and, unlike paper and indelible ink, this source could be modified without leaving a trace. (phase 1 and 2 in Table 1) the advent of time sharing and data communications have allowed continuous access to data from many locations (phase 3) creating access exposures; database systems have added more complexity to auditing due to the lack of obvious mapping between the physical and logical organization of data (phase 4).

Auditors dealt with these changes by (1) tailoring computer programs to do traditional audit functions such as footing, cross-tabulations and confirmations, (2) developing generalized audit software to access information on data files, (3) requiring many security steps to limit logical access in multi-location data processing environments and (4) developing specialized audit computers and/or front-end software to face the challenge of database oriented systems.

However, MIS continue to advance in design and technology. Corporate MIS, and particularly financial systems, are evolving towards decentralization , distribution, online posting, continuous (or at least daily) closing of the books, and paperlessness [Vasarhelyi and Yang, 1988]. These changes are causing additional challenges for auditors and

TABLE 2

Database Systems and their Audit

System Characteristic	Audit (level 1)	Audit (level 2)
Database	Documentation	Data dictionary query
Database size	User query	Auditor query
Transaction flows	Examine levels	Capture sample transactions
Duplicates	Sorting and listing	Logical analysis and indexes
Field analysis	Paper oriented	Software based
Security issues	Physical	Access hierarchies
Restart & Recovery	Plan analysis	Direct access
Database interfaces	Reconciliation	Reconciliation and transaction follow-through

Audit work on these systems is constrained by strong dependence on client system staff (for the extraction of data from databases) and typically entails reviewing the manual processes around the large application system. In traditional system audits these procedures were labeled as "audit around the computer". These procedures, are labeled as "level 1" in Table 2 and are characterized by examination of documentation, requests for user query of the database, examination of application summary data, sorting and listing of records by the user (not the auditor), a strong emphasis on paper, physical evaluation of security issues, plan analysis for the evaluation of restart & recovery and manual reconciliation of data to evaluate application interfaces. Level 2 tasks, described in Table 2, would use the computer to perform database audits as well as eliminate the intermediation by the user or systems people (auditees) in the audit of database systems. This hands-on approach utilizes queries to the data dictionary, direct use of the system by the auditor and would rely on transaction evidence gathered by the auditor using the same database technology. The level 2 approach reduces the risk of fraudulent (selective) data extraction by the auditee and allows the audit to be conducted more efficiently if the auditor is well versed in database management. Furthermore, audit effectiveness is increased because the auditor has greater flexibility in the search for evidence and it is not obvious to the auditee what data are being queried by the auditor (resulting in improved deterrence of fraud). Differences in desired audit approach and the technological tooling necessary for performing level 2 tasks led to the development of some of the concepts used for Continuous Process Auditing.

CONTINUOUS PROCESS AUDITING

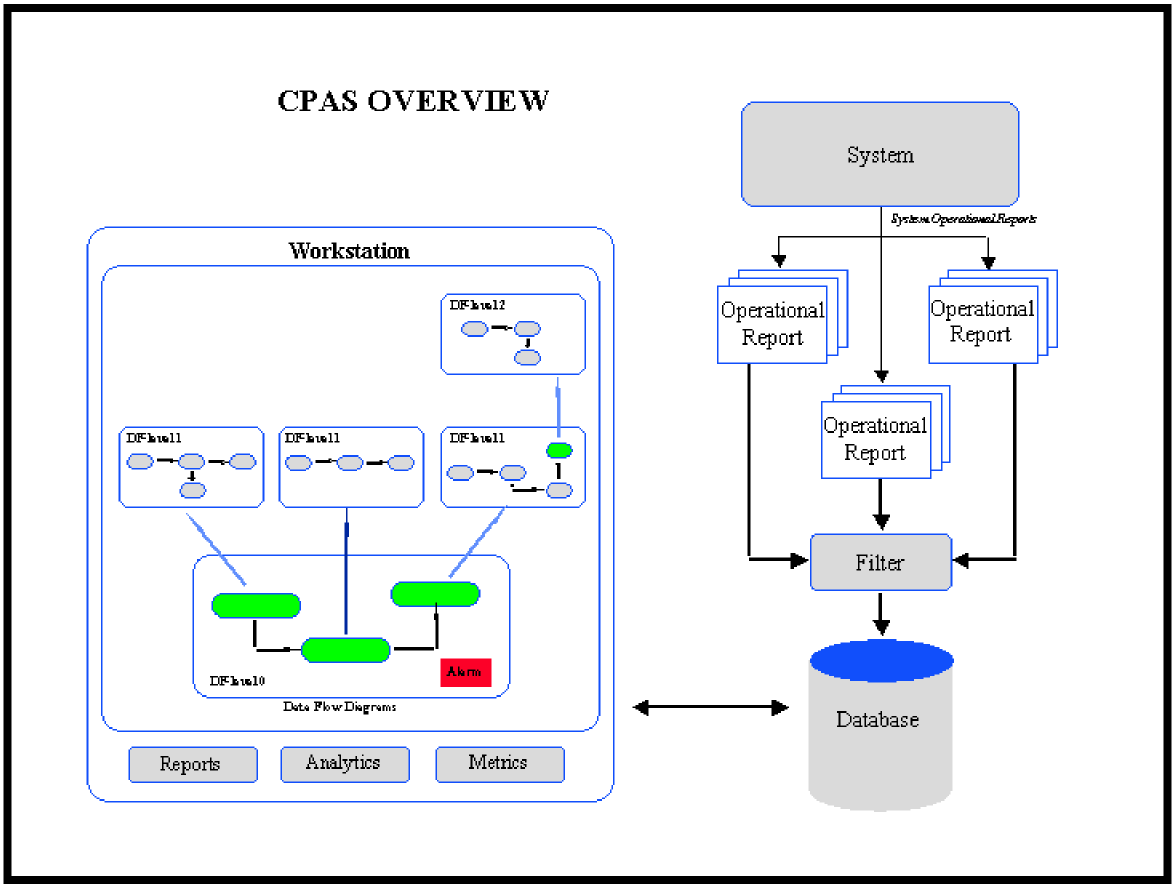
There are some key problems in auditing large database systems that traditional may imply an obtrusive intrusion on the system and can result in performance deterioration. The installation of these monitoring devices must be planned to coincide with natural life-cycle changes of major software systems. Some interim measures should be implemented to prepare for online monitoring. The approach adopted at AT&T, with the current CPAS prototype, consists of a data provisioning system and an advanced decision support system.

Data provisioning can be accomplished by three different, though not necessarily mutually exclusive methods: (1) data extraction from “standard” existing application, reports, using pattern matching techniques; (2) data extraction form the file that feeds the application report; and (3) recording of direct monitoring data. The approach used in CPAS entails first a measurement phase where intrusion is necessary but the audit capability is substantially expanded.

Measurement. Copies of key management reports are issued and transported through a data network to an independent audit workstation at a central location. These reports are stored in raw form and data are extracted from these reports and placed in a database. The fields in the database map with a symbolic algebraic representation of the system that is used to define the analysis. The database is tied to a workstation and analysis is performed at the workstation using the information obtained from the database. The basic elemtns of this analysis process are described later in the paper.

Monitoring. In the monitoring phase, audit modules will be impounded into the auditee system. This will allow the auditor to continuously monitor the system and provide sufficient control and monitoring points for management retracing of transactions. In current systems, individual transactions are aggregated into account balances and complemented by successive allocations of overhead. These processes create difficulties in balancing and tracing transactions.

The AT&T CPAS prototype uses the “measurement” strategy of data procurement. This is illustrated in Figure 1. The auditor logs into CPAS and selects the system to be audited. The front end of CPAS allows the auditor to look at copies of actual reports used as the source of data for the analysis. From here the auditor can move into the actual analysis portion of CPAS. In CPAS, the system being audited is represented as flowcharts on the workstation monitor. A high level view of the system (labeled DF level 0 in Figure 1) is linked hierarchically to other flowcharts representing more detail about the system modules being audited. This tree oriented view-of-the-world which allows the user to drill down into the details of a graphical representation is conceptually similar to the Hypertext approach [Gessner, 1990]. The analysis is structured along these flowcharts leading the auditor to think hierarchically.



Analysis. The auditor's work is broken down into two phases: first, the startup stage where he/she works with developers, users, and others to create a view of the system, abd second, the use stage when he/she actually uses the system for actual operational audit purposes. The auditor's (internal or external) role in this context is not very different from its traditional function.

At the setup stage, the auditor acts as an internal control identifier, representer, and evaluator using existing documentation and human knowledge to create the system screens (similar to flowcharts) and to provide feedback to the designers/management. Here, audit tests, such as files to be footed and extended or reconciliations to be performed, as well as processes to be verified, are identified. Unlike the traditional audit process, the CPAS approach here requires the "soft-coding" of these processes for continuous repitition. Furthermore, at this state, the CPAS database is designed, unlike in the traiditonal process, standards are specified and alarm conditions designed.

In the use stage, the system is monitored for alarm conditions and the alarm conditions are investigated when they arise and the symptoms and diagnostics identified and impounded into the CPAS knowledge base. The current baseline version of CPAS provides auditors with some alarms for imbalance conditions, the ability to record and display time-series data on key variables, and a cries of graphs that present event de-composition.

This logical view of the system can be associated with diagnostic analytics that count the number of exceptions and/or alarms current in the system. Detailed information about *each* main module is available at lower levels through a drill-down procedure. This information is presented primarily as metrics. analytic, and alarms.

Metrics

Metrics are direct measurements of the system, drawn from reports, in the measurement stage. These metrics are compared against system standards. If a standard is exceeded, an alarm appears on the screen. For example, in the auditing of a billing system, the number of bills to be invoiced is extracted from a user report. The number of bills not issued due to a high severity error, detected by the normal data processing edits, is captured as well as the total dollar amount of bills issued. These three numbers are metrics that relate to the overall billing process.

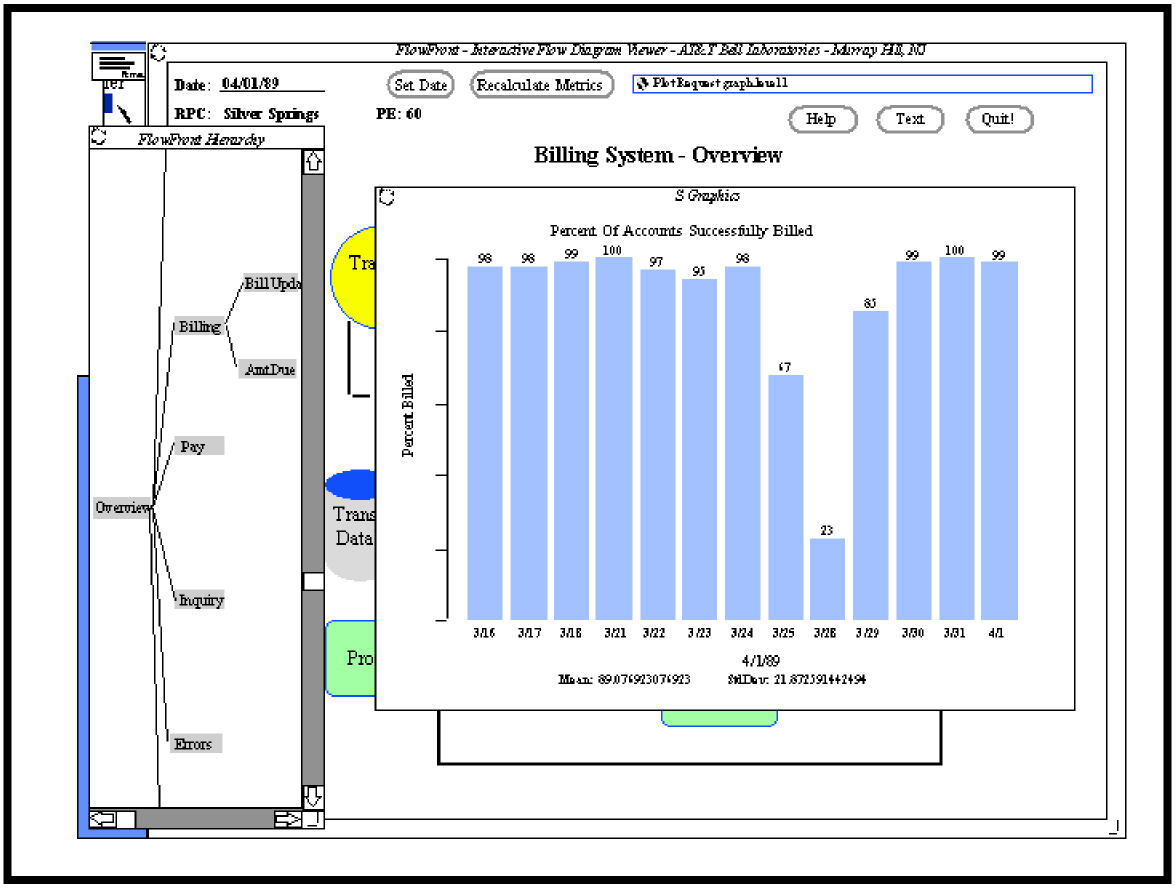
Analytics

Analytics are defined as functional (natural flow), logical (key interaction), and empirical (e.g. it has been observed that ....) relationships among metrics. Specific analytics, related to a particular system module can be derived from the auditor, management, user experience, or historical data from the system. Each analytic may have a minimum of three dimensions: 1) its algebraic structure, 2) the relationships and contingencies that determine its numeric value at different times and situations and 3) rules-of-thumb or optimal rules on the magnitude and nature of variance that may be deemed as “real variance” to the extreme of alarms. For example, a billing analytic would state that dollars billed should be equal to invoices received, minus values of failed edits plus (or minus) the change of the number of dollars in retained invoices. The threshold number of expected invoices for that particular day or week (allowing for seasonality) must be established to determine whether an alarm should be fired.

Alarms. An alarm is an attention-directing action triggered, for example, when the value of a metric exceeds a standard. Actual experience with these issues indicates that *several* levels of alarms are desirable; (I) minor (type I) alarms dealing with the functioning of the auditing system; (2) low-level operational (type 2) alarms to call exceptions to the attention of operating management (3) higher-level (type 3) alarms to call exceptions to the attention of the auditor and trigger 'exception audits:' and (4) high-level hype 4) alarms to -am auditors and top management of serious crisis.

For example, a type I alarm may be triggered if two sets of data are produced by the audited system, for the same module, for the same day, and it is unclear from information given which data to load into the database. Of course, cycle and re-run information should be clearly passed along with the data but sometimes this will not be as clean as expected. A type I alarm might also be triggered if the reports change format and data extraction procedures need to be modified. These Type I alarms will need to be acted upon immediately, usually with a call to the system administrator or system management organization.

A type 2 alarm might be triggered if data pertaining to the same process are inconsistent. For example data from many different reports might he used to perform an intramodule reconciliation. The data must come from different jobs in order for the



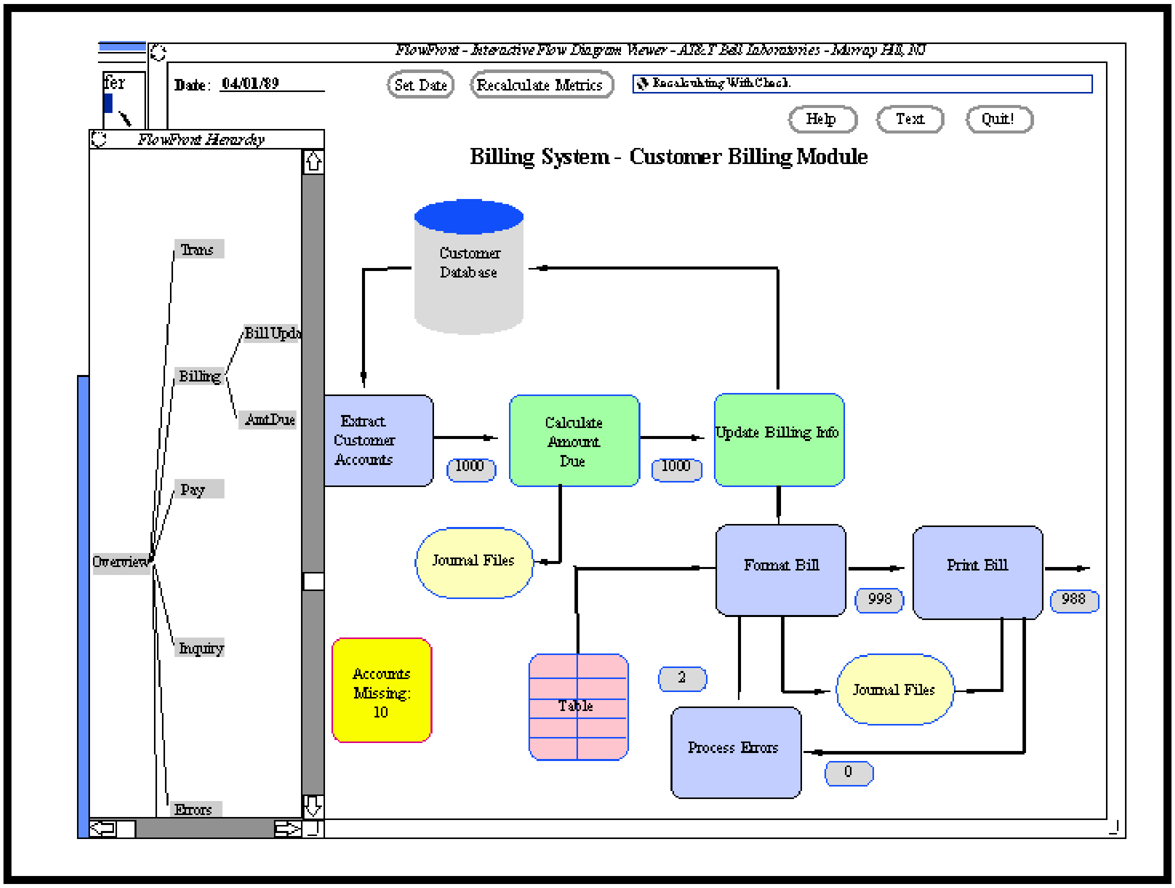
The CPAS application may be testing that the following controls are in place: (1) completeness and accuracy of input; (2) completeness and accuracy of update; (3) timeliness" of data arriving to die system and h timeliness of system processing; (4) maintenance of data in the database; (5) accuracy of computer programs; and (6) reasonableness of the data. For example, the auditor might have defined tests (and had them built into the CPAS application) to answer the following questions:

Were all transactions sent to the biller, received? Can all of the transactions be accounted for? Were all of the trans actions loaded into the Process Transactions module? Were they loaded correctly?

How many transactions were in error? Has the error threshold been exceeded? How long does it take errored transactions to re-enter the system?

Were all transactions posted to the database correctly? Were all the trans. actions initiated, executed, and recorded only once? Can all of the transactions that entered the system be accounted *(or (i.e.,* either on the database or in an *error* file, or rejected back to the source)? How accurate are the data that were loaded to the database (i.e., does the sum of! he dollars on the database match what was to be posted to the database)? Are all databases synchronized?

Were: the bills calculated properly? How reasonable are the amounts billed? Were all customers who *were* supposed to be billed actually billed?



The audit" may wish to look at the history of the reconciliation. Figure 5 is a two level time-series showing the number of accounts lost and the total number of accounts billed for a dive-week period ending 4/l/90.The graph indicates that the out-of-balance condition occurred once at the beginning of the period and again on 4/1/90. M condition appeared to have bun corrected at the beginning of the period, since the reconciliation did not fail again until the current day's processing. The auditor should reset the date to 3/11/90 and check the metrics to determine if the reconciliation failed for the same reason that it did on 4/1/90. This could indicate inadequacy of controls or poor compliance with internal controls. More detailed analytics and we metrics relating to the actual billing process and the interface between this module and other modules in the system are found at different levels. This information, taken together, presents an integrated diagnostic view of the system being audited."

Insert Figure 3

Complementing the actual hands-on audit work is an auditor platform, accessible at any level, which can include a series of different functions. This platform should ultimately contain at least a statistical package, a graphics package, a spreadsheet package (including a filler to the database), a report generator, and a teat editor. These tools can be used for *ad hoc* analysis or be linked to the “wired-in” procedures in CPAS. An even other technological environment may incorporate

CPAM requires long-term monitoring and reaction to emerging evidence, something that, with limited experience, is difficult to manage. Given this, the issue of resistance to change may arise. This can be handled by the issuance of an audit manual that describes how to audit with CPAS and extensive training and technical support for the auditors.

Ideally, management also its version of CPAS, so they are aware when major problems occur in their system. Auditors could browse their own CPAS (with independent analytics) on a periodic basis and follow up on any alarm conditions to see what management has done about them.

Future work on CPAS will focus on increasing the quality of auditor work by integrating the auditor platform with the auditor workstation, increasing the use of monitoring probes, improving the quality of the auditor heuristics, and impounding more expertise into the system.

The introduction of real-time systems require that the auditor be able to attest to the system of internal accounting controls at different points in time. Continuous process auditing can effectively help the auditor to evaluate these controls, but will require substantive changes in the nature of evidence, the types of procedures, the timing, and the allocation of effort in audit

REFERENCES

Alter, S. , Decision Support Systems: Current Practice and Continuing Challenges (Addison-Wesley Publishing Company, 1980).

Bailey, A. D., G. L. Duke, G. E. Gerlach, C. E. Ko, R. D. Meservy and A. B. Whinston, "TICOM and
the Analysis of Internal Controls," The Accounting Review,
(April 1985), pp. 186-201.

---and R. D. Meservy, P. E. Johnson, "Internal Control Evaluation:
A Computational Model of the Review Process," Auditing: A Journal of Practice and Theory, (Autumn 1986), pp. 44-74.

---and K. Hackenbrack, P. De and J. Dillard, "Artificial
Intelligence, Cognitive Science and Computational Modeling in
Auditing Research: A Research Approach," Journal of Information
Systems1 (Spring 1987).

---and L. E. Graham, and J. V. Hansen, "Technological
Development and EDP" in
Abdel-Khalik, A. R. & Solomon, I. "Research Opportunities in Auditing: