

University of Mississippi

eGrove

Proceedings of the University of Kansas
Symposium on Auditing Problems

Deloitte Collection

1-1-1986

Discussant's Response to "Impact of technological events and trends on audit evidence in the year 2000: Phase I"

Rajendra P. Srivastava

N. Allen Ford

Follow this and additional works at: https://egrove.olemiss.edu/dl_proceedings



Part of the [Accounting Commons](#), and the [Taxation Commons](#)

Recommended Citation

Auditing Symposium VIII: Proceedings of the 1986 Touche Ross/University of Kansas Symposium on Auditing Problems, pp. 147-151;

This Article is brought to you for free and open access by the Deloitte Collection at eGrove. It has been accepted for inclusion in Proceedings of the University of Kansas Symposium on Auditing Problems by an authorized administrator of eGrove. For more information, please contact egrove@olemiss.edu.

Discussant's Response to "The Impact of Technological Events and Trends on Audit Evidence in the Year 2000: Phase I"

Stephen M. Paroby
Ernst & Whinney

My compliments go to authors Holstrum, Mock, and West for a well-written and well-thought-out paper and a project that will have a significant impact on all of us. Mark Twain once said, "It's all right to make predictions, but not about the future." Technological forecasting tends to be optimistic in the short run and pessimistic in the long run. Had this paper been written in 1970, I truly wonder if it would have predicted today's environment. However, the authors have taken a compilation of speculations that are often difficult to quantify or fully support and put them in a perspective that will certainly jar today's auditor.

Computerized systems benefit all of us in several ways. Computers process transactions with much greater consistency than is possible in a manual system. In addition, the speed and flexibility of computer processing provide wide-ranging capabilities for a timely, reliable reporting of high volumes of information. These capabilities give management greater opportunity to make informed business decisions and allow management to react quickly to and capitalize on business developments.

As the number of on-line systems and paperless transactions continue to increase, new products will continue to emerge to provide auditors with more sophisticated computer-assisted audit techniques. Advancing technology such as micro-to-mainframe communications, down-loading of information from centralized or decentralized sites, expert systems, and artificial intelligence probably will not change basic audit techniques of review and verification. What this technology will change significantly is the way auditors evaluate and test systems. The traditional approach of examining "hard" copies is neither adequate nor feasible. Computerized techniques have been developed to deal with this task. Various software programs and utilities can provide exception reports and other audit-related information. Embedded audit modules can select and verify all or a sample of transactions and generalized audit software performs calculations faster and much more accurately than we could manually. However, the consistency, speed, and flexibility of the computer can pose additional control concerns for us as auditors. These concerns include:

1. The effect of errors may be compounded. For example, the computer may prepare sales invoices by taking the quantity input and extending it by price on the sales price master file. If the program is not functioning properly (e.g., selecting incorrect prices,

- performing extensions improperly), all sales invoices may be incorrect.
2. The reduction of manual involvement resulting from the presence of the computer in the process could lead to inadequate segregation of duties.
 3. Audit trails may be reduced or eliminated, or may exist for only short periods of time in computer-readable form.
 4. Changes to data and programs may be made by individuals lacking a sufficient understanding of the overall system of internal control and standard operating policies. Also, such changes may be made without adequate testing by a quality assurance group or without the consent of management.
 5. More individuals may have access to data, a critical corporate resource. These individuals may be authorized or unauthorized. Authorized access could still lead to either errors or irregularities, and unauthorized access usually leads to computer fraud.

As recently reported by the FBI, computer fraud ranges from three to five billion dollars annually. The average return to the perpetrator in reported crimes has been calculated at \$615,000, quite a difference from the \$23,000 average for manual embezzlements. As evidenced by these figures, computers can greatly facilitate the misappropriation of assets and the manipulation of information under certain circumstances.

Therefore we should keep in mind that while a computer's involvement in the accounting system or in a production process often has a positive impact, this does not necessarily mean the data it generates are correct, nor that adequate controls are in place. In most cases, control procedures will exist. However, we need to identify and test them before relying on them, just as we would in a manual system.

Also, all auditors will have to increase their understanding of computerized systems. In order to plan and execute an audit effectively, auditors will have to determine the impact of the computer on the data they are examining. In addition, they will have to gain an understanding of the controls over the processing of the data. Specifically, this will include controls over the development and maintenance of programs and controls over access to data files and programs.

Having painted the picture of what the future that is here today holds, let me focus on some of the significant changes in information technology and the paper presented by the authors. Essentially, the authors take current technology and project it forward, anticipating no new significant technological break-throughs. Clearly, in an area evolving as rapidly as computer technology, such an approach could be risky. For example, had this paper been written ten years ago, the authors may have failed to predict the revolutionary impact of microcomputer technology.

I agree with the authors that the micro-to-mainframe links and local area networks will become much more common. In addition, these links and networks will present control challenges. The more difficult task will be to predict how these technological trends will affect auditing. A clear distinction should also be made between big, unusual transactions and little, normal ones. Although the authors state that three of the currently strongest forms of

evidence—physical examination, confirmation, and vouching—could possibly all deteriorate in reliability and persuasiveness, it is unclear now whether other forms of evidence—or other types of audit procedures—will be able to compensate for these potential losses.

Computer-based information is intrinsically more reliable than printed information. Perhaps the most important effect of new computer technology will not be in a reduction in the quality of audit evidence, but a greater emphasis on computer controls to assure its accuracy and the avoidance of unwarranted reliance on computer-generated data.

Audit failures usually result from not understanding a particular transaction or class of transactions and the related processing and control systems rather than because the inventory listing does not foot. New information technology is not likely to alter this situation but in fact may compound it.

When you relate the changes in information technology that will affect future audit evidence and the impact of those changes on auditing, certain issues come to mind. Some of the specific issues that should be addressed include:

1. How to make computer technology and computer tools accessible to general auditors. In broad terms, audit evidence is what auditors examine. If auditors cannot understand computer technology, computerized files will not be considered audit evidence.
2. It seems likely that analytical review will become the centerpiece of most audits within ten years. An important aspect of increased computer technology is that clients can now accumulate and analyze a much larger amount of information than previously possible. That information makes possible much more detailed and persuasive analytical reviews. Also, through the use of artificial intelligence, more information will be gathered, synthesized, and put into useful form faster than ever before.
3. Audit coverage will increase dramatically. For example, when we test inventory extensions manually, we typically select a small sample of inventory items to recompute. If we use software tools to check the same computation, we generally test all inventory items. As we move toward more computerized auditing, the percentage of transactions we examine will increase. If we had to do it manually, audit fees would be astronomical.
4. The authors cite Weber and suggest that generalized audit software may be unavailable to run on microcomputers and minicomputers for many years to come. At Ernst & Whinney we are now using a multimachine generalized audit software package that runs on a microcomputer, as well as microcomputer software that gives us the ability to extract data from essentially any minicomputer or mainframe. That technology is here today.

Given the rapid change in technology in just the last few years, it will be almost impossible to project what the computerized auditing environment will be in the year 2000. Aside from the obvious concerns and those already mentioned (e.g., data security, lack of audit trails), some additional pervasive considerations are (1) what financial statements will look like 10 to 20 years from now and how financial information will be distributed and (2) how audits will be performed then.

Regarding presentation of financial information, several questions come to mind. For example, will shareholders and other financial statement users have continuous access (via their own computer terminals or other devices) to a company's financial information? Will audits be done entirely by computers from the auditor's office, in which case "field work" would virtually disappear except for some inquiries and observations?

Another major question is how the sophisticated technology of the future will affect the structure of CPA firms and the staffing of audit engagements. A related issue is the impact on accounting and business schools. Accounting students will need to have a much more detailed background in information systems before joining a CPA firm, and the firms themselves will need to provide increased training to supplement normal development programs. We have recently released an interactive computer-based training course, *EDP Concepts for Auditors*, designed to raise the level of computer literacy for all auditors.

How will smaller CPA firms adapt? The impact of technological change generally is not felt as quickly by the smaller firms, since their clients tend to be the last ones to adopt sophisticated technology. However, in 10 to 20 years even small businesses likely will place substantial reliance on the computer. Accordingly, the smaller firms will need to invest in the necessary hardware and software to keep pace with their clients and the rest of the profession. This increased sophistication definitely will place more emphasis on the system of internal controls. Companies will need to turn increasingly to EDP managers to make sure that adequate control systems are installed and then to their auditors for assurance that the controls are functioning.

Better communication between external and internal auditors would seem to be a necessity for coping with the changes in technology. The authors refer to "continuous control auditing." Not only would this cause us to place more reliance on internal audit, but it would seem to change dramatically the nature and timing of our tests. The authors state that "Changes affecting the nature and availability of audit evidence are occurring so rapidly that auditors have difficulty making practical plans to gradually adopt their auditing techniques and processes to deal effectively with future forms of audit evidences." Frankly, what we are doing now in terms of researching and testing new hardware and software and training personnel seems to be the appropriate course of action. Although long-range planning is important, we can realistically look only to the short term because of the rapid advancement of technology.

With tomorrow's technology here today, management's and audit committees' concerns about the computer are intensifying. Management and audit committees are increasingly asking their auditors to provide answers to such questions as: What information is being processed on our computer; why; for whom; by whom? What would happen if our computer system went down for a day, a week, or a month? What would happen if our key data processing personnel left tomorrow? Can someone with a telephone and a home computer access our confidential files? Within our organization, can only people with the need to know gain access to confidential data? Are there proper segregation-of-duty policies? To answer these and other questions effectively, it is imperative for all auditors to be more computer literate.

As an auditor, how do you respond when you ask the data processing manager how things are going and he replies:

I had just arrived in town to bring the on-site on-line. No sooner had I brought it up than it went down. Rising to the occasion, I went downstairs and gathered my tool kit: Time Domain Reflectometer, logic probe, comm lube, and spare low-order bits.

Going to the SOURCE, I TC'd the packet with some spare protocols until the EtherLink locked up TSO and broke the SYSGEN. I slipped a Turbo Accelerator into the PC and revved it up until it executed an infinite loop in under three seconds.

Coming in the back door under VMS, I broke the UNIX shell and released the ASCII characters in the error traps. Applying CSMA/CD brought the recovery rate safely below the BIOS buffer overflow. DOS recovered, and the crisis was over. . . .

Many of the skills previously reserved for a few high priests in the data processing center are now required of all of us.