NEED FOR MORE AND BETTER COMPUTER AUDITING

BY

ELLSWORTH H. MORSE, JR.
ASSISTANT COMPTROLLER GENERAL OF THE UNITED STATES

AT THE
FOURTH ANNUAL FALL SEMINAR
AND
FIRST ANNUAL REGIONAL SEMINAR
OF THE
NATIONAL CAPITAL AREA CHAPTER
EDP AUDITORS ASSOCATION
WASHINGTON, D.C.

OCTOBER 13, 1977

The technical challenges that face management officials whose systems include electronic computers and their auditors who must satisfactorily cope with those systems almost defy description. The objectives sought have not changed--accurate and prompt processing of data and production of usable and useful information for operational and management control purposes. Tied in with these broad objectives is the need to protect the security of processed information and prevent fraud in any form.

Auditors confronting such systems have no real choice but to be technically equipped to test the workings of the management's information and control systems and to recommend improvement or correction of any serious problems encountered--actual or potential.

These homely truths are easy for speechmakers to state. But, achieving them is widely recognized as a most difficult

task. That is one reason why seminars such as this one are important. They provide an excellent forum for the exchange of information about automated data processing resources and systems and the information they produce and about auditing methods and techniques.

In our work in the General Accounting Office in reviewing the nature and effectiveness of management control systems and internal auditing in the Federal agencies, we see an urgent need for auditors to not only do more about computer auditing but also improve greatly the quality of the auditing they are now doing. For this reason, a seminar can also serve to help auditors, who may be hesitant or a bit fearful about auditing in the computer environment, to learn from the experience of others.

In GAO, we place great emphasis on having auditors on our staff who have the capability to audit automated systems, be these systems in the financial, operational, personnel, logistics, or other management areas. We have no choice. The systems are there and must be examined.

In the executive agencies of the Federal Government, with their vast inventory of computers, the tremendous annual cost of operating them, and the growing dependence of managers--at all levels--upon computers and their output products for the management of major programs, agency auditors must play a vital

role in helping assure management that the computer systems are working effectively, are producing accurate and reliable reports, and are under adequate control. The role of the General Accounting Office, as a legislative branch agency, is to evaluate these systems and promote whatever changes are necessary to make them as effective as possible.

The questions you are asking today, "Can management rely on auditors' reports in those areas where the computer is involved?" and further, "Can the public itself depend on these assurances?" are most important. They go to the heart of a long-established system of checks and balances in which auditors have had a key role. What is really being asked here is, "Has the 'mystique' of computer systems reduced the auditors' effectiveness?" I believe we should welcome such questions and then address them forthrightly.

It is in the formulation of answers to these questions that we can demonstrate that there really is no mystique in computer systems. We merely find a different and tougher technology to cope with. There is a shift in the skills and understanding needed to audit these systems. The challenge to auditors is one of hard work, acquisition of specialized experience, new and demanding training, and an ability to shift to using the computer itself as a tool for carrying out audit procedures.

However, nothing in all this changes the fundamental principles of the auditor's profession. The question remains, "Have auditors in general met this challenge?" In the Federal Government, we in GAO do not feel that enough is being done by auditors in the area of computer auditing.

The integrity of computerized systems continues to be the target of much public criticism. Certainly, one purpose of auditing computer systems is to give management officials and policy makers information on whether the systems are reliable and correctly produce or summarize the data processed. Further, these officials should demand such information. Auditors cannot avoid a measure of accountability when computer systems lack controls, are used inefficiently, or uneconomically, or are tools for criminal activity.

We are all well aware that the use of computers continues to reach into every area of our society. Each of us, whether we like it or not, is becoming more and more dependent upon and affected by computers and automated systems. Those of you from the banking community are very concerned with the questions and challenges presented by the electronic transfer of funds.

How are auditors preparing to cope with these problems? How do we cope with the point-of-sale systems which are steadily increasing? How do we do our job in service bureaus

that support large numbers of clients and where our task may just involve a small part of that operation? The speakers who follow in this seminar will help provide some answers to these specific questions. I think the key question, however, is one we must ask ourselves; that is, "Are we as individuals ready for these challenges?"

Have we as auditors made that personal commitment to acquire the new knowledge, new experiences, and new skills that we know are needed to respond to these challenges? Your sessions here will certainly identify some of the new knowledge and new skill areas. I hope you will use them as a source of information to guide your own planning to prepare yourself.

Within the Federal Government, more than 10,000 computers are now in operation, and the best estimate we have is that annual ADP costs exceed $10 billion.

Perhaps of more significance than the dollar amount expended for these services is the impact they have on Federal programs and activities. The Government's decisions resulting from computer-produced information is evident through the accomplishments made in such diverse fields as space exploration, agriculture, housing, transportation, nuclear energy research, and large-scale clerical and accounting operations. It seems inevitable that Federal

managers will continue to rely even more heavily on computer systems in solving complex problems and for managing large programs and resources.

Because of their importance costwise, as well as from the standpoint of impact on the programs and activities in which they are used, automatic data processing systems must be subjected to independent review and evaluation to find out whether they are reliable and to identify ways and means to improve them. The very magnitude of ADP costs, together with existing and potential problem areas, compels evaluating the impact of ADP on programs, operations, and resource use. Auditors should be helping top management find out whether these resources are used efficiently, managed effectively, and are producing reliable and accurate information and reports.

But, our work in GAO reveals that too many audit organizations have avoided examining computer systems and applications. In our most recent report dealing with computer auditing in the executive departments released just last month--there is a copy in your seminar material--we pointed out that there is a long history of Federal agency audit organizations' aversion to work involving computers and computer-based applications. We have noted that this aversion was present in the private sector as well as

in the Federal Government. The problem probably exists at State and local government levels as well.

Does the auditor who avoids the computer--or attempts to audit around the computer--meet accepted audit standards? The answer has to be a resounding "no."

Our report concluded that not enough computer auditing was being done by executive-branch agency auditors, and it presented several recommendations to agency heads and their audit organizations for actions to strengthen this most important element of management control. In more personal terms, here is how we think individual auditors should look at what they are doing.

First, on every job, he should ask himself, "Will the computer-produced data have an influence on my findings?" If the answer is yes and he does not pursue the trail into the computer (wherever it goes), then he is avoiding the computer. Sometimes these risks are taken to keep audit costs down, but he should know that the risks include having questions raised on the integrity of his work--the very theme of this seminar.

Secondly, the auditor should identify the types of ADP audit tasks that he might be confronted with in the next 3 years or so and then identify the ADP knowledge and skills he will need to perform these tasks professionally. This may

seem like an unimportant step, but it is perhaps the most important one he can take. The computer field is so wide that he could attend courses indefinitely and still not be focusing on his real needs as an auditor. He should invest his training time wisely and aim for specific results from the training. Otherwise, he and his employer may find themselves getting frustrated and turned off because of unwise training choices.

With respect to compliance with auditing standards, the GAO "Standards for Audit of Governmental Organizations, Programs, Activities & Functions" states:

> "If the audit work requires extensive review of computerized systems, the audit staff must include persons having the appropriate skills. These skills may be possessed by staff members or by consultants to the staff."

The need for auditors to develop their technical competence and perform work in the computer area is further brought out by the recent report of the Institute of Internal Auditors on systems auditability and control.

Among the principal conclusions of that study were the following:

- Internal auditors must participate in the system development process to insure that appropriate audit and control features are designed into new computer-based information systems.

--Controls must be verified both before and after installation of computer-based systems.

--As a result of the growth in complexity and use of computer-based information systems, needs exist for greater internal audit involvement relative to auditing in the data processing environment.

--An important need exists for EDP audit staff development because few internal audit staffs have enough data processing knowledge and experience to audit effectively in the data processing environment.

--Many organizations are not adequately evaluating their audit and control functions in the data processing environment. Top management should initiate a periodic assessment of its audit and control programs.

In today's environment, good audits of computers and automated applications require technical competence far beyond that required of auditors in the past. The time is long gone that auditors can both ignore the existence of the computer and successfully discharge their responsibilities. Again, referring to what I said earlier, we as auditors must take the needed actions to acquire the

necessary technical skills and knowledge to successfully audit in the computer environment. Without these capabilities, our work will be substandard, and those who rely on such audits will be misled. Inadequate work in this area can badly damage the auditor's reputation for reliability and competence.

I do not wish to convey nothing but gloom and doom to you, however. Many audit organizations have the capability to do excellent computer auditing, and many of you are trying to further your capabilities.

But, in many audit organizations, a structured, long-range approach is needed to bring internal auditors to the point where they can deal effectively with computer systems and applications. To achieve the desired level, top management must provide strong direction to auditors to develop a program for appropriate involvement and periodic reporting of progress made.

CATEGORIES OF COMPUTER AUDITING

Computer auditing can be divded into two broad categories.

One category consists of auditing what is done by a computer--in other words, auditing a computer application. An example would be a review of an automated accounts payable system. Such an audit might well encompass the adequacy

of controls over input data, over the integrity of the computer's processing, and over computer output products.

The second type of computer auditing is much broader and goes far beyond the computer itself. This type involves examining questions such as the following:

--Is the system properly designed?

--Is there a valid requirement for the system or application?

--Is the computer being operated efficiently?

--Are the system procedures documented properly, and are they up to date?

--Are the functional users satisfied with the output products?

--Is the computer configuration appropriate for the work to be performed?

--Are all personnel (ADP as well as functional staff) adequately trained for operation and use of the system?

Both types of computer auditing are within the area of responsibility of the internal auditor who is responsible to management for helping assure that operations are being carried out economically, efficiently, and effectively in accordance with the directives of management. But, as I have already indicated, however, we have observed that too

many internal audit groups shun ADP auditing, particularly the second or broader aspect.

AUTOMATED DECISIONMAKING

To illustrate the need for closely scrutinizing ADP applications, let me briefly describe the outcome of one of our computer audits.

About a year ago, we released a report entitled "Improvements Needed in Managing Automated Decisionmaking by Computers Throughout the Federal Government." In our audit work at a naval installation, we observed that certain types of stocks in an automated inventory system were building up, though they should not have been. After some digging, we discovered a quirk in the computer program which had the effect of double counting requests for issuance of parts and supplies. Naturally, the computer ordered replacements automatically to accommodate this apparent increase in the need for such parts and supplies. But the result was that unneeded stock was ordered.

No one had questioned the computer's output. Before we looked into the cases, the computer's actions were assumed to be correct. Our auditors worked to get the situation remedied. Then we began to wonder how frequently other situations of this type might exist where a computer's input was resulting in actions being taken automatically--actions that could be wrong--with no review by human beings.

We reviewed the reports of other internal audit agencies within the Government to find out whether similar situations had been encountered elsewhere. These reports provided us the answer in a short time. We were surprised to find that it was rather common for internal auditors to encounter automated systems turning out bad decisions--decisions not being detected by operators and users of the system. The internal auditors had unearthed the errors in automated systems, had run them down, and had corrective actions taken. But--and here is the important point--each of these had been treated as an individual case when, in fact, there was a pattern of such bad decisions. Eventually, we were able to attribute these similar cases to bad programing, bad data, or a combination of the two. These factors, together with almost unquestioning acceptance of the outputs of computers as correct, had resulted in losses amounting to hundreds of millions of dollars through erroneous payments, ordering unneeded items, incorrect eligiblity determinations, and the like.

By establishing that this pattern existed rather generally across the Government, and in disclosing the magnitude of the errors being made, we were able to convince the Office of Management and Budget of the need to issue specific directives to all Federal departments and agencies

directing them to take the broad corrective steps recommended in our report.

One of the most important of these steps is the provision for internal auditors to make periodic reviews of the output of automated systems to see whether the decisions being made are correct. Another is to encourage early auditor involvement in the development of such systems to make sure that appropriate controls and audit trails are built in. This report has made an important contribution to improving the use of computers in the Federal Government and to demonstrating the need for continued, careful surveillance by internal auditors of computer systems.

CURRENT COMPUTER AUDITING PRACTICE

In our more recent report on computer auditing that I mentioned earlier, we cited several examples of the avoidance of computer work by audit organizations. We also found in our review that some agencies have developed the capability to perform computer audits. True, the capabilities vary widely among the departments and agencies, but nevertheless, we learned that, where such capability had been developed, excellent--even spectacular--audit results have been reported.

We reported that some internal audit groups in the Federal Government are conducting critical and searching analyses of ADP resources, determining the effectiveness of automated systems, and assessing the adequacy of the ADP functions to meet users' needs. We also learned that ADP auditing covers a wide spectrum in the departments and agencies. Our report described or cited examples of computer auditing work in the areas of system design and development, equipment acquisition, ADP installation management, and specific applications.

AIR FORCE EXAMPLE

One of these audits was performed by the Air Force Audit Agency. It reviewed proposed system concepts, supporting rationale, and documentation for an automated management information system. Matters considered included the adequacy of objectives in relation to user needs, cost reliability, and whether technical requirements were valid.

The auditors determined that user needs, system capabilities, and resources had not been substantiated in the original requirements document. Technical and equipment specifications were not substantiated by adequate studies, and users indicated there was little need for the proposed online data base.

The original economic analysis--which identified the estimated costs and benefits--was inaccurate and unsubstantiated, according to the auditors. Further examination disclosed that the projected manpower reduction, comprising most of the projected savings, was not realistic.

This audit resulted in a major change in the scope, equipment, and personnel requirements for the system. The revised requirements, approved at just under $5 million, reflected a cost avoidance directly attributable to the audit of over $31 million.

Of course, computer audits will not always provide such spectacular results. This is true of all auditing. This example also illustrates that in the automatic data processing area, as well as in many other areas, the auditor can often make an important contribution by getting involved before final decisions are made.

THE PROBLEM OF FRAUD

Before closing, let me bring out one other problem--and that is detecting the ever-present possibility of fraud. Fraud is a broad term covering many kinds of sins, but in essence, it amounts to unlawfully separating people or organizations from money or resources that rightfully belong to them.

Federal auditors have to keep a wary eye out for this possibility at all times. The advent of computer techniques and systems has not lessened their concern or responsibility in any way. In fact, it has probably made it worse.

Those of you who read The New Yorker magazine saw the recent lengthy article by Thomas Whiteside on this subject. His very readable article made it clear that our society includes many who are quite willing to tackle the technical challenge of mastering the workings of computer systems to divert money or other resources unlawfully for their personal use.

GAO sent a report to the Congress a little over a year ago summarizing quite a number of computer fraud cases in the Federal Government. These cases had been brought to light through agency checks and audits--not by GAO--but the point of the report was that managers and auditors have to be alert all the time to test their systems to detect fraud and tighten them when fraud is found to prevent it in the future.

The general public--the man or woman in the street--may know little or nothing about the technicalities of computers or internal management controls. But when they read about frauds involving the long, undetected stealing

of money by milking an organization's system, computer-based or not, the most likely question to be raised in their minds first will be, "Where were the auditors?"

Auditors cannot escape accountability for weak accounting and control systems. This is true even though primary responsibility for strong systems rests with management. Management officials have the job of designing and installing good systems to start with and including all necessary measures to prevent fraud. Internal auditors support those highly laudable objectives through testing, evaluating, and reporting on their findings. The computer age has not changed this lineup in basic responsibilities. It has only made the job technically harder to perform.

CONCLUDING OBSERVATIONS

We have seen auditors who knew little or nothing about computers become highly skilled in a relatively short time by concentrating on the knowledge and techniques in which expertise was needed.

We have also seen people trained in the computer sciences acquire the audit skills needed to perform expertly as auditors.

Thus, it is possible for audit organizations to acquire the expertise they need. With that expertise, they should have the confidence to tackle the difficult job of examining the computer systems in their agencies. And, by doing so, they can demonstrate to management officials that they are on top of their job and are better prepared to constructively assist those officials in discharging their responsibilities.

In closing, let me refer once again to the recent GAO report on computer auditing. Management officials and auditors in the Federal agencies--and elsewhere--should review it carefully and ask themselves whether the shoe fits. They should ask themselves whether they are doing enough auditing of their systems. If they conclude that they are not doing enough, they should then be able to recognize the risks that they are taking. I would hope that such recognition would in turn lead them to take the vigorous and decisive actions needed to shore up a serious weakness in their internal management control systems.