EDP ANALYZER

JUNE, 1977
VOL. 15, NO. 6

THE IMPORTANCE OF EDP AUDIT AND CONTROL

The use of computers in business is now in its third decade. Most medium and larger size organizations are heavily automated, particularly for their financial applications. One would expect that EDP control procedures (for protecting the integrity of the data) and audit procedures (for verifying results and evaluating those controls) would be widely understood and practiced. Unfortunately, this is not the case. The Institute of Internal Auditors has just published a landmark study that deserves the attention of executive management, EDP system designers, and internal auditors. Here is an overview of the importance of the subject and what the study has reported.

To set the stage for this discussion of EDP audit and control, we will address a series of questions.

Question: What is EDP auditability and control? As defined in the Institute of Internal Auditor's study (Reference 1), systems control pertains to the mechanisms within a total systems environment that ensure the accuracy and completeness of the information within the system and in its output. Auditability refers to the features and characteristics of the system needed to verify (1) the adequacy of the controls and (2) the accuracy and completeness of the outputs.

Question: Why are these important? Controls are needed to insure the accuracy, completeness, and integrity of the information within the system. The system may contain financial data, operational data, company-proprietary data, and/or personal data about people. Audit is needed to verify that the controls are being used effectively and that the outputs are accurate and complete. A comprehensive audit program that includes both of the elements just mentioned can provide assurance that historical data is correct and that future processing results have a degree or reliability.

Question: What attention is being given to EDP audit and control? In general, far too little attention is being given to these subjects. Executive management tends to turn the responsibility for computer-based systems over to data processing management. Data processing management is more concerned about getting the application systems to perform the desired functions, and about computer center efficiency, than about system controls. Controls for financial application systems do receive attention, of course, but the amount of attention often depends upon the individuals involved. Internal auditors too often see their responsibilities as relating to systems where information is recorded on paper, not computer-based systems. In other words, they tend to "audit around" the computer by checking some outputs, without attempting to verify the controls used in the computer programs and data processing operations.

Question: How serious is the need for EDP audit and controls? The need for carefully designed controls often is not appreciated until a severe difficulty or loss occurs due to the lack of controls.

True, most organizations recognize the need for at least basic internal controls for handling financial data. Management recognizes the risk of loss due to errors, thefts, and so on. Both internal and external auditors look for basic internal controls and report on their absence or ineffectiveness.

But the need for controls in systems that handle operational data, company-proprietary data, or personal data is not as well appreciated. Apparently, losses in these systems due to the lack of controls have not been of sufficient size or consequence to attract the attention of top management.

The seriousness of the need for controls, then, seems to be measured by the losses that have occurred and that have been detected. Further, good information about such losses is hard to obtain. Organizations naturally are reluctant to publicly discuss cases of waste or theft that they have detected. So here is the dilemma. Executive management probably will not get too concerned about the need for enhanced EDP audit and controls until substantial losses are reported. And organizations that detect such losses tend not to publicly report those losses, if they can avoid it. So it is the organizations that have detected such losses that give the subject the attention it deserves.

There is one source of information on losses due to inadequate controls, however. This source is several reports prepared by the U.S. General Accounting Office (GAO), Reference 2. These reports have been prepared for the Congress and are matters of public record. The referenced reports deal with cases of waste occurring from poorly designed automated decision making procedures (such as inventory reordering), from losses due to computer-related crime, and from losses due to physical damage to computer installations.

Before describing the case examples in the reports, two main points should be made. One is that these cases represent only part of the control and audit problem; they necessarily deal only with detected cases. One might also question whether these cases, taken from U.S. federal government experiences, are sufficiently representative of problems in other types of organizations. Stanford Research Institute, in a report prepared for GAO, gave the opinion that the opportunities for computer crime in federal programs and private industry are about the same. It is possible that the same statement might also be made about poorly automated decision-making procedures and computer site safety safeguards.

The other point is that we do not wish to overemphasize computer-related crimes. Auditors, both internal and external, stress that the main goal of internal controls in financial systems is to safeguard the assets from waste due to errors, and to insure the accuracy and completeness of financial statements. Auditors do not claim that internal controls will detect fraud or embezzlement. However, good internal controls and good audits of those controls, while they may not prevent improper activities, tend to discourage such activities.

Let us now consider some relevant experiences in U.S. federal government agencies.

Errors in automated decision making

In Reference 2a, it is reported that federal agency computers cause more than 1.7 billion payment authorizations, checks, bills, requisitions, etc. to be made out each year, totalling some $44 billion, without anybody reviewing or evaluating whether they are correct. With this volume of automated decision making, errors can quickly turn into huge losses of money. Several cases were discussed.

In one U.S. Army system, requisitions for shipment of inventory items to overseas locations were prepared by a computer. The decision of which stocking point the shipments were to be made from were made by the computer. Analysis showed that the decision procedure did not first check to see if a shipment could be made from the stocking point which was nearest to the destination. The result was that many shipments were made from more remote stocking points, resulting in unnecessary transportation costs. The audit agency estimated that these unnecessary costs were in the order of $900,000 per year, and that the excess inventory investment (due to the longer transportation pipelines) amounted to about $1.3 million.

In a U.S. Navy system, an automated procedure was used for scheduling the overhaul of aircraft spare equipment. The scheduling procedure used had errors in it—errors that resulted in duplication of requirements, overstatements of material usage, and premature overhaul. The auditors

estimated that the effect of these errors was millions of dollars in unnecessary costs. Navy officials did not agree with this figure but they did agree that the problems existed.

A Veterans Administration system prepared monthly payments to some 185,000 veterans for apprenticeship and other on-the-job training programs. Auditors found that the system did not have adequate validation of input transactions, allowing incomplete transactions to be entered. When the program found the data to be missing, it used a default procedure involving "standard" values. This procedure caused overpayments in the order of $700,000.

The audit agencies involved cited several main causes for these errors in automated decision making. For one thing, the programs used incomplete, inappropriate, or erroneous decision making criteria; this was reported in 30 of 32 cases studied. Another shortcoming was that the decision making logic was not what the user requested, as reported in 24 of the cases. The systems omitted needed validation checks, allowing incomplete transactions to be processed by resorting to default procedures, in 11 cases. Data elements were found to be incomplete, incorrect, or obsolete in 49 cases. These data errors were due to the use of complex forms that confused users, to the lack of instructions and training for the people filling out the forms, to the lack of review of the data, and to workload pressures due to high volumes of transactions.

GAO solicited opinions of how to prevent or reduce such problems by sending out questionnaires to 600 people who were members of some computer-field professional societies. Replies were received from 263 people. Some of the main recommendations made were the following.

Documentation should exist that highlights the automated decision making criteria and related critical data elements, as well as validity checks. A pre-implementation review of an automated decision making system should be made by qualified auditors or others who are independent of the designers and users. This review should evaluate the decision making logic, criteria, and validity checks. Also, a post-implementation review should be made as soon as possible after the new system has been put into operation, to see how it is working in practice. Thereafter, some method should be used for monitoring the automated decision making process on a cyclical basis. Finally, prime responsibility should be assigned to a single point for insuring the quality of data—including responsibility for proper internal controls, instructions and training for the people who prepare the data, good forms design, and so on.

Computer-related crimes

GAO contacted nine federal agencies within the Departments of Agriculture, Justice, HEW, and others, which had reported 74 cases of apparent computer-related crimes. Of these, 69 met GAO's definition of a computer crime. GAO investigated 12 of these cases in depth and talked to perpetrators in three of the cases.

In the 69 cases that GAO considered computer crimes, losses totalled over $2.1 million. In at least 50 of the cases, the crimes were performed by system users, not data processing personnel. Of the 69 cases, 27 involved fraudulent direct payment of funds, while another 28 involved fraudulent inventory or supply actions. In eight cases, personnel records were altered without authorization. In another four cases, computer facilities were used for personal benefit, and in two cases, operations were sabotaged.

The most common type of computer crime is where the perpetrator enters fictitious transactions which, for example, cause checks to be created and mailed to accomplices. In the case of one welfare system, fraudulent welfare checks were sent out to the tune of somewhere between $90,000 and $250,000; the auditors were unable to pinpoint the losses any closer than that.

GAO pointed out that federal managers are responsible for establishing effective internal controls to safeguard assets. This action is required by legislation and by supporting directives. But based on this study, said the GAO, management does not place sufficient emphasis on the internal controls. A higher priority is assigned to making the application system operational and a lower priority to assessing and minimizing potential risks.

As far as improvements in internal control systems are concerned, GAO said that better separation of duties may be the greatest single need. The second most pressing need noted is better physical control of facilities and supplies.

Improvements are needed in EDP audit techniques, GAO stated. In 5 of the 12 cases studied in

depth, auditors had not reviewed the controls in the systems involved. In four other cases, investigative officials other than auditors had reviewed the controls, but only after the crimes had been detected. In 13 of the 57 other cases rated as computer crimes, audits or special reviews did result in the discovery of improper actions.

Stanford Research Institute performed a special study for GAO, relating federal computer crimes to those uncovered in private industry. Most such crimes are uncovered accidentally, said SRI, due to the perpetrator making a mistake or such. The "typical" perpetrator is young, between 18 and 30 years of age, said SRI. Further, he or she is highly motivated, intelligent, personable, a good worker and generally not unhappy with his job, employed for several years with no history of job problems, trusted in his work environment, and possibly over-qualified for his job. This seems to be a description of the type of employee that management seeks to hire. What causes the problem? The usual reason, says SRI, is a short-term financial problem. The employee turns to theft to solve the problem temporarily and then gets in the habit of stealing.

GAO's recommendations included the following, to help reduce computer crimes. Develop an organization plan that provides an adequate separation of duties. Set up procedures to properly control assets, liabilities, revenues, and expenses. Establish a system of practices for each duty and function. Install a system of effective internal controls. And if crimes are detected, analyze them in order to determine weaknesses in the management control process that made them possible.

Shortcomings in physical protection

GAO representatives visited 18 federal processing installations in the U.S. and 10 overseas. They observed protection procedures for equipment and for valuable data, and used a checklist to see what measures were and were not being used.

The most common general type of failing was in the area of fire hazards. The next most common failing involved flood and water hazards, followed by possible sabotage and possible theft or misuse.

In addition, GAO contacted 23 other installations in the U.S., some of which were known to have had physical protection problems. The purpose here was to find out just what the costs and other impacts of physical damage might be. Again, some cases of fire and flood damage resulted in losses of millions of dollars, as well as substantial efforts to get the installations operating smoothly again.

GAO's recommendation was that management officials be appointed at each installation with responsibility for physical security and risk management. Federal guidelines are already available for instituting such programs. While not mentioned in the GAO recommendations, we suspect that GAO would agree with us that EDP auditors should include physical security and risk management factors in their audits.

Observations on the GAO studies

In this brief summary, we have been able to touch on some of the main points of the GAO reports. We suggest that they be studied in more detail.

It seems to us that the GAO studies support the view of some experts in the computer security field. This view is that the greatest magnitude of loss will come from errors of omission and commission. Losses due to theft and losses due to physical damage follow. The losses due to theft attract the most attention perhaps. But it is the system errors and inadequate internal controls that, over a period of time, account for the bulk of the losses.

Perhaps the GAO reports might be accused of being self-serving by stressing the need for audits, since GAO plays an audit role—but we would not agree with this accusation. We think that an effective set of system controls and an effective EDP audit program would go a long way toward reducing waste due to errors and losses due to physical damage. We suspect that controls and audits also will deter some (but not all) perpetrators of crimes.

We should also mention at this point that EDPACS (Reference 5) frequently provides summaries of reported computer abuses and crimes. In the March 1977 issue, for instance, three detected cases of computer abuse and one suspected case are reported. An alleged inventory fraud case may involve as much as $40 million in losses. In the suspected case, a man earning $23,000 a year had three wives and families in three cities, a fiance in another city, and a private plane for get-

ting around the country. His job was that of supervising the installation of automatic teller terminals in banks.

We return to our earlier question: how serious is the need for EDP audit and control? Based on the experience of the U.S. federal government, and the cases reported in EDPACS, we conclude that the need is serious indeed. The types of problems encountered by the government agencies are the types of problems that can confront any computer user. The potential losses can be measured in large amounts of money.

It is timely, then, that the Institute of Internal Auditors (IIA) has just issued a series of three reports on system audits and controls.

The systems auditability and control study

The IIA systems auditability and control (SAC) study had its beginnings in mid-1974, when William Perry joined IIA as its Director of Research. He had spent the previous 15 years at Eastman Kodak, and had been involved both with data processing and with internal audit.

Members of two key IIA committees expressed the view to Perry that an "audit" should be performed to see how well auditors were doing their job as related to EDP. It was the belief of these members that EDP audit was not being adequately performed, and they felt that an objective study was needed to find out just what was happening. So Perry was given the assignment to determine how to proceed.

Perry himself talked to a number of individuals and companies, to get ideas on the scope and method of conduct of the study. The more people he talked to, the broader the scope became. It soon was clear that the study costs would exceed IIA's resources for such a project, if the study was going to be performed by an independent organization. So Perry also contacted the major computer manufacturers about financial support for the project. Several said that they would cooperate. But IBM did more than that. After careful consideration, it agreed to provide a grant of $500,000 for the study.

The study was organized with three main objectives in mind. First, it was desired to find out just what was happening in the area of EDP audit and control among leading organizations. Not what these organizations were thinking of doing but what they were actually doing. IIA felt that the study results might have a significant impact on the design of future data processing systems.

The second main objective was to increase management's focus on the need to build better controls and auditability into computer-based systems, and to gain management support for the controls and auditability deemed necessary by auditors and EDP personnel. And thirdly, it was desired to put control and auditability into the proper perspective within the total systems environment.

It was also decided that two other areas would *not* be singled out for particular attention—because there were people already working on these subjects and a large amount of written material is already available. These were the areas of security and computer crime.

With these objectives agreed upon, IIA solicited proposals from twelve research organizations. Proposals were received from four of them. And in March 1975, Stanford Research Institute was selected to perform the study.

The study got underway in April 1975, with the appointment of an advisory committee with 47 members. These members came from the U.S., Canada, and Western Europe. The committee included representatives from the major data processing associations, accounting associations, and CPA firms, as well as people from GUIDE, SHARE, user companies, interested government agencies, and academic institutions. The role of the advisory committee was to submit ideas for the conduct of the study and to act as a sounding board for the tentative results and conclusions. A basic groundrule was that if a member of the advisory committee did not agree to have his name associated with the project, he could have his name removed from the list of advisory committee members. In actuality, all 47 members stayed with the project during the two years of the study and, upon review of the final reports, all of them agreed to have their names on the reports.

In addition, a 4-person steering committee was formed to provide the executive guidance needed during the conduct of the study. This committee consisted of the chairmen of two IIA committees, Perry, and a representative from IBM. IBM's main interest was to make sure that an objective study was performed and that schedule and budget were met, we were told. One aspect of objectivity requested by IBM was that users of all

major brands of computers be included in the study.

Finally, a 6-person technical review committee was formed. It was a subset of the advisory committee. This technical review committee was to be in close touch with the project as reports were being developed. Committee members were to provide a critical review of the reports before those reports were submitted to the full advisory committee.

The first step in the study itself was a mail survey of 500 U.S. companies. The intent of this survey was to help define the field of study. From the replies, it was decided to concentrate on organizations spending $22,000 or more per month on data processing equipment rental. It was in such organizations, project members concluded, that the more meaningful audit and control practices were likely to be found.

The next step was a questionnaire directed at executives of a selected sample of organizations meeting the above criterion—that is, $22,000 or more per month rental. Again, a sample of 500 organizations was selected. A commercial file of computer field installations was used, in order to obtain representative coverage. A random sample of 261 organizations was selected from the population of regulated industries, and a random sample of 239 organizations was chosen from the non-regulated industries. One week before questionnaires were mailed out, an "advance letter" was sent to the chief executive officer of each organization, informing him about the nature of the study. Then three questionnaires—one for executive management, one for the director of data processing, and one for the chief auditor—were sent to this same executive for him to pass on to the appropriate people. Follow-up letters were sent ten days later. Of the 500 organizations contacted, 283 responded.

In addition, SRI contacted by mail almost 100 federal and state agencies, and almost 600 organizations in Canada, Europe, and Japan.

A telephone survey was conducted among 100 non-responding organizations in the main U.S. survey. Selected questions were asked, to determine if systematic differences existed between the respondents and non-respondents.

Next, a list of more than 300 organizations was proposed by the advisory committee, as candidates for in-depth interviews. This list was reduced to 175 by discussions between SRI and IIA, in an attempt to get good representation by industry groups and company size, and to avoid duplications of the audit techniques that were studied. SRI then telephoned these organizations, to ask about their control and audit techniques. Based on the responses, 75 were identified as potentially desirable to visit. Of these, 45 were ultimately visited by SRI project members, in the U.S., Canada, Europe, and Japan.

Major contributions of the study

We talked to key participants in the project at IIA and SRI, and to Malin E. See, who was the SRI project director, about what they thought were the major contributions of the study. So, before we get into a description of the study results themselves, here is how these key participants view those results.

First definitive study. These participants see the SAC project as the first definitive study of EDP audit and control that addresses three main audiences. Three separate but related reports address the interests of executive management, EDP system designers, and internal auditors. Each report is written in the language of its audience. Further, each report gives the appropriate level of detail for its audience on what control and audit practices are actually being used, based on an extensive study of organizations in the U.S., Canada, Europe, and Japan.

Top management interests. The SAC project has taken the position that the initiative for more effective EDP audit and control should come from the top of an organization. So the executive report aims to get top management more interested in and more concerned about EDP audit and control. If the report is successful in instilling this interest, a major contribution will have been made, these key participants told us.

Control aspects. The control report is directed at the interests of EDP system designers. It is written not only in their language but also uses a frame of reference with which they are familiar. Over 200 control techniques that are used in practice are described. Four case studies show how selected groups of these control techniques are being used in four organizations. System designers can immediately begin incorporating some of these control techniques in new system designs, we were told.

major brands of computers be included in the study.

Finally, a 6-person technical review committee was formed. It was a subset of the advisory committee. This technical review committee was to be in close touch with the project as reports were being developed. Committee members were to provide a critical review of the reports before those reports were submitted to the full advisory committee.

The first step in the study itself was a mail survey of 500 U.S. companies. The intent of this survey was to help define the field of study. From the replies, it was decided to concentrate on organizations spending $22,000 or more per month on data processing equipment rental. It was in such organizations, project members concluded, that the more meaningful audit and control practices were likely to be found.

The next step was a questionnaire directed at executives of a selected sample of organizations meeting the above criterion—that is, $22,000 or more per month rental. Again, a sample of 500 organizations was selected. A commercial file of computer field installations was used, in order to obtain representative coverage. A random sample of 261 organizations was selected from the population of regulated industries, and a random sample of 239 organizations was chosen from the non-regulated industries. One week before questionnaires were mailed out, an "advance letter" was sent to the chief executive officer of each organization, informing him about the nature of the study. Then three questionnaires—one for executive management, one for the director of data processing, and one for the chief auditor—were sent to this same executive for him to pass on to the appropriate people. Follow-up letters were sent ten days later. Of the 500 organizations contacted, 283 responded.

In addition, SRI contacted by mail almost 100 federal and state agencies, and almost 600 organizations in Canada, Europe, and Japan.

A telephone survey was conducted among 100 non-responding organizations in the main U.S. survey. Selected questions were asked, to determine if systematic differences existed between the respondents and non-respondents.

Next, a list of more than 300 organizations was proposed by the advisory committee, as candidates for in-depth interviews. This list was reduced to 175 by discussions between SRI and IIA, in an attempt to get good representation by industry groups and company size, and to avoid duplications of the audit techniques that were studied. SRI then telephoned these organizations, to ask about their control and audit techniques. Based on the responses, 75 were identified as potentially desirable to visit. Of these, 45 were ultimately visited by SRI project members, in the U.S., Canada, Europe, and Japan.

Major contributions of the study

We talked to key participants in the project at IIA and SRI, and to Malin E. See, who was the SRI project director, about what they thought were the major contributions of the study. So, before we get into a description of the study results themselves, here is how these key participants view those results.

First definitive study. These participants see the SAC project as the first definitive study of EDP audit and control that addresses three main audiences. Three separate but related reports address the interests of executive management, EDP system designers, and internal auditors. Each report is written in the language of its audience. Further, each report gives the appropriate level of detail for its audience on what control and audit practices are actually being used, based on an extensive study of organizations in the U.S., Canada, Europe, and Japan.

Top management interests. The SAC project has taken the position that the initiative for more effective EDP audit and control should come from the top of an organization. So the executive report aims to get top management more interested in and more concerned about EDP audit and control. If the report is successful in instilling this interest, a major contribution will have been made, these key participants told us.

Control aspects. The control report is directed at the interests of EDP system designers. It is written not only in their language but also uses a frame of reference with which they are familiar. Over 200 control techniques that are used in practice are described. Four case studies show how selected groups of these control techniques are being used in four organizations. System designers can immediately begin incorporating some of these control techniques in new system designs, we were told.

Audit aspects. The audit practices report is directed at the interests of internal auditors. Again, it is a definitive study of what EDP audit practices are actually being used, described in the language and framework that auditors know. The report describes in detail 28 audit techniques, with examples of the use of each. And again, auditors can begin to use some of these techniques immediately, we were informed.

Communications bridge. The control and audit reports discuss common material but from the viewpoints of system designers and internal auditors. These reports therefore provide a communications bridge between these two groups. One of the main difficulties that the project encountered in its field study was the lack of communication between these two groups.

Verifying controls. The three reports make a clear distinction between reviewing the adequacy of controls, verifying the controls, and verifying the results of processing (the output data). This distinction has not always been fully appreciated by auditors in the past. Verifying the results of processing is not equivalent to verifying the controls nor to determining the adequacy of the controls that are used in the processing procedures.

Observations on the study

The key participants that we talked to also made several observations about the study.

As just mentioned, an important finding was that data processing personnel and internal auditors often do not communicate well. These two groups may have different meanings for the same terms. Literature and guidelines written for one group may be considered unusable by the other group. If the project reports do, in fact, provide a communication bridge between these groups, they will have made a significant contribution.

EDP audit is still considered a specialty within internal audit, at essentially all organizations contacted. But with the bulk of these organizations having their financial and operational records on the computer, EDP audit should become part of the mainstream of internal audit, and not just a specialty within internal audit.

All too frequently, the EDP audit tools available to internal auditors, and the training in the use of these tools, are not sufficient nor adequate. The majority of tools and techniques are not adequate even for auditing batch systems, to say nothing of more advanced systems involving data bases, data communications, distributed processing, and so on.

Lastly, it was pointed out that there are three other publications that, together with the SAC reports, provide a broad coverage of EDP audit and control. Each of these publications supplements the others. Two of these publications are reports prepared by the Canadian Institute of Chartered Accountants (Reference 3), on computer control guidelines and computer audit guidelines. These two reports provide a conceptual framework for audit and control, as contrasted with the IIA/SRI study of the practices used in the field. They were perhaps the first publications to structure the whole area of EDP control objectives and techniques. The third publication is a book on computer control and audit (Reference 4), prepared by three partners of Touche Ross & Co., and published by IIA. This book highlights risks and exposures and provides a preventive perspective. One of its goals is to provide some structure to the EDP function itself so that designers can select controls appropriate to the situation and auditors can select audit techniques appropriate to both the EDP function and the controls. So References 1, 3, and 4 should be in the library of every EDP auditor, it was emphasized to us.

Executive report

As mentioned above, project members concluded that the initiative for better EDP audit and control should come from executive management. So a 20-page executive report was prepared, to explain to top management about the study and its major recommendations.

This report points out management's continually growing need for information, coupled to the hazards of inadequate audit and control. More and more information is being carried in automated systems. If controls on the quality and completeness of that information are inadequate, then the repercussions can be widespread.

The report addresses eight main areas. These are: management responsibilities, the need for improved control, participation by internal auditors in system development, verification of controls, the need for improved internal auditor involvement, EDP audit staff development, and the need for improved EDP audit tools and techniques.

The report concludes with a brief description of the cost implications of systems audit and control.

One point mentioned to us was that essentially no thorough cost/benefit analyses had been performed on EDP audit and control practices, either by data processing personnel or by auditors, in the organizations contacted during the study. Such analyses would not be easy, because they would have to deal with potential losses resulting from inadequate audit and controls. While there was a belief that total system costs would be reduced by improved controls, there was no way to clearly substantiate that belief. One of the benefits that should accrue from the publication of the GAO studies (Reference 2) is a better appreciation for the losses that can occur when controls are inadequate.

Control practices report

As mentioned, this report primarily addresses the interests of EDP system designers. It discusses the control techniques that are being used during application system development, application system operation, and in computer service center operations.

Also as mentioned above, SRI sent questionnaires to executive management, data processing managers, and internal auditors. Each group was asked to rank their concerns about EDP audit and control. While there were different relative concerns expressed by the three groups, the main concerns of all three groups were: errors and omissions, improper controls, and inadequate system design.

Even though all three groups indicated concern on these and other points, there was no clear agreement on who was responsible for overseeing the installation and use of internal controls. Responsibility tended to be fragmented. Internal controls associated with manual procedures tend to be the responsibility of line management. But if a computer is involved, user department line management tends to turn the responsibility over to data processing personnel. Concern about controls tends to be limited mainly to accounting and financial applications. Even in these types of applications, controls are often viewed from a narrow perspective rather than from the overall application system and its associated control objectives.

As mentioned, controls are discussed from the standpoint of application system operation, application system development, and computer service center operation. We will start with controls for application system operation.

Application system controls

How does a system designer go about incorporating an adequate set of controls in a new application system? The following approach might well lead to an effective use of controls.

First, the selection of the controls to be used should be made early in the development cycle. The selection should be made in the context of the total application system and its control needs. In theory at least, the selection should be based on explicit management policies concerning control, organization structure and the separation of duties, plans for guiding efforts and for measuring achievement, and operating policies and procedures. In practice, these overall policies are not fully formulated. So the system designer should talk to a number of people who are likely to be the most interested in and concerned about the controls for the system.

After the control mechanisms have been selected and incorporated in the new application system, a pre-installation review and test should be made—to see if the selection has been adequate and if the controls seem to be effective. Generally, user department and data processing department personnel test the new system before conversion, to make sure that it functions as it should. These are usually the same people who designed and developed the system. From the standpoint of reviewing and testing controls, it would be preferable for this to be done by an independent group that includes internal auditors. Further, it is quite important that the internal audit function be independent of the user departments and the data processing department.

After the new system has been installed, a post-installation review should be made to test the effectiveness of the controls in practice. Any errors or shortcomings in the controls should be detected and corrected as soon as possible, before such shortcomings can lead to much damage. Finally, the control procedures used in the manual parts of the system should be verified.

Both the control and the audit reports use a common structure for the flow of transactions

through an application system. This structure has seven components. The first component is the transaction origination activity, which generally is under the control of user departments. Then come five components under the control of data processing—transaction entry, data communications, computer processing, and data storage and retrieval. The last step is output processing, which is partially under the control of the users.

Following are the main types of controls associated with each of these seven components.

Transaction origination controls. Five generic types of controls apply to transaction origination—source document origination, authorization, input preparation, source document retention, and source document error handling. In these five categories, 45 specific control procedures are discussed. For instance, under source document origination, a sub-type of control involves source document design which in turn includes special-purpose forms, source document preprinted sequential numbers, and type of transaction identification. Each of these is discussed in a separate paragraph, ranging from two to ten sentences in length.

We should emphasize that these are control procedures that are in actual use. Each application system would use a selected subset of these controls for transaction origination, depending upon the needs, risks, and costs. As an example, a written authorization for a transaction might be appropriate for transactions affecting negotiable resources, but not appropriate for routine job flow transactions in a production plant.

Transaction entry controls. These controls contain the following generic types: batch data entry, on-line terminal data entry, data validation, batch proof and balancing, and error handling. A total of 36 specific types of controls are described. One example is the use of a pre-formatting with on-line terminal data entry, to guide the terminal operators in supplying the input data.

Data communications controls include message input controls, message transmission controls and message reception and accounting controls. A total of 32 specific control types are described.

Computer processing controls. Two generic types of controls are identified—process integrity and error handling. Examples of process integrity controls are the use of transaction codes and the use of control totals. In all, 24 specific controls are discussed.

Data storage and retrieval controls include file handling controls and file error handling controls. File handling controls, in turn, are made up of library controls, file access controls, file maintenance controls, and backup procedures. File error handling includes error reporting, error correction, and correction reentry. A total of 31 controls are discussed.

Output processing controls. Six generic types are identified, including balancing and reconciliation by data processing personnel, output distribution, balancing and reconciliation by user personnel, accountable documents, and output error handling. There are 33 control types discussed.

So the application system controls section of the control report discusses over 200 specific control procedures which are based on the practices in the firms contacted by SRI.

Computer service center controls

We are attempting to give the flavor of the control and audit reports by briefly listing the types of controls and the types of audit procedures that the study encountered in its field work. We are also attempting to convey thereby our impression of an extensive list of control types and audit practices.

The real usefulness of this control material will come, of course, when a system designer uses the control report to help identify the types of controls that should be used in a new application system he is designing. That usefulness will have to come from the report itself. It is impossible in an overview such as this to do more than to indicate the merit of the report and to urge system designers to study it.

The computer service center controls are divided into eight generic types: input-output scheduling and control, media library controls, malfunction reporting and preventive maintenance, environment controls and physical security, separation of duties, resources planning, user billing and charge-out procedures, and disaster recovery procedures.

Some of these tend to overlap with application system controls, as in the case of input-output controls. Others are largely independent of the specific application systems, as in the case of disaster recovery procedures.

A total of 52 specific control types are discussed in this section of the report.

Application system development controls

The report points out that the adequacy and effectiveness of controls in application systems are affected by the methods and procedures used in the development process. Controls over system development are important for three reasons. First, they assist in managing costs and schedules. Second, they help insure that appropriate controls are built into the application systems. And third, they ensure that those controls will be properly tested before the application systems are put into operation.

The controls used in controlling the development process tend to follow the steps in the development process. The controls break into seven generic types: system development life cycle controls, project management, structured programming, acceptance testing, program change control, documentation, and data base administration. A total of 39 specific controls are discussed.

We were intrigued by the term "structured programming" being listed as a generic type of control. The point being made by the report is that structured programming provides specific guidelines to programmers on how they may use a programming language and how each program fits together to form an application or operating system. As such, it can be considered as a control discipline on the building process—which at the same time, would help to make the programs more auditable.

Adequacy of control list

The list of controls in actual use was developed from SRI's field interviews and mail surveys. The question then arose: how well does this list work in practice? If some actual systems are studied, will important omissions be found in the list?

So four application systems were studied to determine just what controls were actually used. These four cases were: (1) an on-line accounts receivable system in a large manufacturing organization, with over 1,000 transactions daily, (2) an on-line order entry system in a large continuous process manufacturing company, with over 3,000 transactions daily, (3) an on-line inventory management system at a large manufacturing company handling over 80,000 line items, and (4) a point-of-sale credit approval system at a large retailer handling over 65,000 transactions daily.

One conclusion from these case studies was that no control types were used that had not already been included in the list. Secondly, some gaps appeared to exist in the control systems. These were reviewed with the managements of the companies. In each case, the managements stated that, in their opinion, the benefits did not justify the cost of implementing those particular controls.

While there is no claim that the list of controls is exhaustive, the project members felt reassured from the fact that no controls used in these four cases were not on their list. Also, the test cases indicated that the list was organized in such a manner that it aided in pinpointing potential gaps in the internal control systems.

Audit practices report

The first four chapters of the control report and the audit practices report are the same, except for the last few pages of chapter 4. This was intended to provide a common communications bridge for systems designers and internal auditors. Of course, in the later chapters of the audit report, details are given of particular interest to auditors.

Since it is not required that auditors read the controls report (although they are certainly encouraged to do so), introductory material is given to explain EDP auditing to the auditor. Also, one chapter deals with the question of developing an EDP audit staff.

Then the report lists and describes the 28 audit tools and techniques that the study found to be in practical use. These 28 tools and techniques are divided into the following seven generic types: audit planning and management, testing computer controls, selection and monitoring of data processing transactions, verification, analysis of computer programs, computer service center evaluation, and application system development evaluation.

In an overview, about one paragraph is used to describe each of the 28 tools and techniques. An example of a technique is a test deck, for testing the control features of a computer program. In some instances, the study found that guidelines and checklists were used by the auditors for performing their checks. Due to the number of

checklists encountered and the need not to identify particular organizations, these checklists are not included in the report (nor are references given as to where auditors might obtain such information). We believe that such information would be helpful for auditors just getting started in EDP audit. Of course, it is common practice for auditors to extend and modify such checklists as they conduct audits and find where changes are needed. But someone else's checklist can be a helpful place to start.

SRI made a survey of the relative use of the various EDP audit tools and techniques. The five most commonly used methods, for both development and production systems, are the following: (1) generalized audit software packages, (2) identify the flow of transactions and associated application controls through manual processes as well as through computer processes, (3) the use of test data, such as test decks, (4) parallel operations, and (5) tagged transactions.

The report then illustrates the use of these 28 tools and techniques by discussing, in one chapter each, which of them are being used for auditing application systems, application systems development, and computer service center operations.

Auditing application systems. The report describes the same seven-component structure of the flow of transactions that is given in the control report. To reiterate, these components are: transaction origination, transaction entry, data communications, computer processing, data storage and retrieval, and output processing.

The audit report then describes the main control points in this transaction flow and indicates which of the 28 tools and techniques auditors are using to verify and evaluate the controls at each of these points.

Auditing application system development. The report discusses how the auditor might check and evaluate the following: statements of user requirements, development standards and guidelines, project management, documentation, acceptance testing, post-installation review, and program change control.

Auditing computer service centers. Eight control areas that the auditor should evaluate are identified. Three of these relate to application systems controls: input-output controls, media library controls, and separation of duties. The other five are general controls: environment controls and physical security, disaster recovery, malfunction reporting and preventive maintenance, resource planning, and user billing and charge-out procedures.

Details on tools and techniques

Up to this point, the report has established a firm communications bridge between the auditor and the system designer. The same control points and types of controls are discussed in each report.

The audit report now gets into a detailed discussion of each of the 28 audit tools and techniques. One whole chapter is devoted to each of these, for a total of over 200 pages for all 28.

As an example, the chapter on the use of generalized audit software has the following sections: (1) overview, (2) typical set of steps to follow in using generalized audit software, (3) application examples, (4) limitations and contraints, (5) implementation considerations, such as package selection, data processing department support that is needed, audit staff training, and costs, and finally (6) evaluation of effectiveness.

To recapitulate: in considering the questions of control and audit of computer-based application systems, the control report and audit report both present the same structure for the flow of transactions through an application system. The control report lists and describes over 200 specific control techniques that are in practical use in applications systems, organized around the major control points. This list should be immediately useful to a system designer in helping select which controls should be used in a new application system he is designing—and to auditors for reviewing and evaluating controls. The audit report looks at an application system in terms of these same control points. It presents details on 28 audit techniques that are in practical use for verifying the existence of controls and evaluating their effectiveness.

In our own experience, many system designers that we have talked to have either ignored the internal auditors altogether when designing new applications systems, or have turned to the auditors for advice on how to build controls into the system. Neither approach is right, as far as we are concerned. We believe that the internal auditors should be one of the groups contacted when the system designer is selecting what controls to use. Finally, a set of controls will have to be selected,

based on risks, threats, and costs. These controls may be more or less than what the internal auditors suggested—but at least the internal auditors have been heard. Then, during pre- and post-installation reviews and tests, the auditors should have a chance to test the adequacy of the controls.

While the advice of the internal auditors should be solicited during the control selection phase, the internal auditors should not design the control system. This step seems just as bad to us as ignoring the auditors completely. The auditors should be an independent group—independent of system design and building. The role that the auditors should play is to review and test the control decisions made by others.

It seems to us, then, that the IIA/SRI project on system auditability and control has presented something very useful for both system designers and internal auditors. The designers have a well-organized list of controls that are in practical use today, from which they can select the controls appropriate for a given application system. While not conclusively proved, there is some evidence that this list is quite comprehensive. So the system designers can select a suitable set of controls without either ignoring the internal auditors or depending too heavily on them. The internal auditors, in their turn, have been provided with a discussion of how 28 practical audit techniques are being used today in EDP audits. This is not meant to imply that, without some computer training, they can jump right in to EDP audits. Rather, to the limit of their EDP knowledge, they can begin using these tools and techniques for auditing current systems, new system development, and computer center operations.

Conclusions

How serious is the need for EDP audit and control? One really needs a series of objective cost/benefit studies that measure the benefits and costs of control and audit practices. Putting numbers to these things is difficult. Control attempts to prevent undesired events from happening; audit checks on the effectiveness of the controls. If controls are installed, how many undesired events do they prevent from happening—and what would have been the costs to the organization if those events had happened? To what extent do controls reduce the need for reruns? How much do they reduce the need for correcting errors?

One way to approach answers to such questions is to study the costs that other organizations have encountered when such undesired events actually did occur. At least such figures give some idea of the magnitude of the possible costs, but probably not the likelihood of such costs occurring.

One of the benefits of the GAO reports (Reference 2) is that they provide some idea of the costs that the U.S. federal government has incurred from inadequate control systems. If other similar studies could be made publicly available, over a period of time, it might become possible to estimate what magnitude of cost an organization could incur from an inadequate set of controls.

As more and more of an organization's information resources are put on the computer, the chance of accidental or deliberate loss increases. We think that the IIA/SRI reports, developed under a grant from IBM, will be very helpful to both system designers and internal auditors for reducing the chance for accidental or deliberate loss.

REFERENCES

1. Systems Auditability and Control Study reports, published by The Institute for Internal Auditors (249 Maitland Avenue, Altamonte Springs, Florida 32701), April 1977:
   a) See, M. and T. S. Eason, "Executive Report," 32 p, price $12.
   b) Fitzgerald, J. M., T. S. Eason, and S. H. Russell, "Data Processing Control Practices Report," 150 p, price $12.
   c) See, M., T. S. Eason, S. H. Russell, and B. Ruder, "Data Processing Audit Practices Report," 190 p, price $12. (Note: all three reports may be obtained for $30. Air mail postage: Mexico and Central America, $6; Europe and South America, $10.50; Asia and Far East, $15.)
2. Reports prepared for Committee on Government Operations, U.S. Senate; available from Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402:
   a) "Problems associated with computer technology in federal programs and private industry, computer abuses," June 1976, 448 p, price $3.95.
   b) "Computer security in federal programs," February 1977, 298 p, price $2.80.
3. Reports prepared by the Canadian Institute of Chartered Accountants (250 Bloor Street East, Toronto 5, Ontario, Canada; in U.S., order from IIA, address above):
   a) "Computer Control Guidelines," 135 p, price $12.50.
   b) "Computer Audit Guidelines," 318 p, price $23.
4. Mair, W. C., D. R. Wood and K. W. Davis, *Computer Control & Audit*, published by IIA (address above), 1976, price $20.
5. *EDPACS*, The EDP Audit, Control and Security Newsletter, published by Automation Training Center, Inc. (11250 Roger Bacon Drive, Reston, Virginia 22090). Price, $48 per year in U.S., $56 (via air mail) in other countries.

It is still too often the case that computer-based application systems are developed behind schedule, over cost, do not do as much as promised, and do not satisfy their users. After twenty years of concentrated attention, why do these troubles continue to arise? A good part of the answer to this question is: because the requirements for these application systems were never stated accurately and completely in the first place. If the requirements statements are erroneous or incomplete, how can the resulting application systems be expected to perform satisfactorily? At long last, this problem area is beginning to receive the attention it deserves. Next month, we will discuss some important progress toward "getting the requirements right."

SUBJECTS COVERED BY EDP ANALYZER IN PRIOR YEARS

1974 (Volume 12)

Number

1. Protecting Valuable Data—Part 2
2. The Current Status of Data Management
3. Problem Areas in Data Management
4. Issues in Programming Management
5. The Search for Software Reliability
6. The Advent of Structured Programming
7. Charging for Computer Services
8. Structures for Future Systems
9. The Upgrading of Computer Operators
10. What's Happening with CODASYL-type DBMS?
11. The Data Dictionary/Directory Function
12. Improve the System Building Process

1975 (Volume 13)

Number

1. Progress Toward International Data Networks
2. Soon: Public Packet Switched Networks
3. The Internal Auditor and the Computer
4. Improvements in Man/Machine Interfacing
5. "Are We Doing the Right Things?"
6. "Are We Doing Things Right?"
7. "Do We Have the Right Resources?"
8. The Benefits of Standard Practices
9. Progress Toward Easier Programming
10. The New Interactive Search Systems
11. The Debate on Information Privacy: Part 1
12. The Debate on Information Privacy: Part 2

1976 (Volume 14)

Number

1. Planning for Multi-national Data Processing
2. Staff Training on the Multi-national Scene
3. Professionalism: Coming or Not?
4. Integrity and Security of Personal Data
5. APL and Decision Support Systems
6. Distributed Data Systems
7. Network Structures for Distributed Systems
8. Bringing Women into Computing Management
9. Project Management Systems
10. Distributed Systems and the End User
11. Recovery in Data Base Systems
12. Toward the Better Management of Data

1977 (Volume 15)

Number

1. The Arrival of Common Systems
2. Word Processing: Part 1
3. Word Processing: Part 2
4. Computer Message Systems
5. Computer Services for Small Sites
6. The Importance of EDP Audit and Control

(List of subjects prior to 1974 sent upon request)

PRICE SCHEDULE

The annual subscription price for EDP ANALYZER is $48. The two year price is $88 and the three year price is $120; postpaid surface delivery to the U.S., Canada, and Mexico. (Optional air mail delivery to Canada and Mexico available at extra cost.)

Subscriptions to other countries are: One year $60, two years, $112, and three years $156. These prices include AIR MAIL postage. All prices in U.S. dollars.

Attractive binders for holding 12 issues of EDP ANALYZER are available at $6.25. Californians please add 38¢ sales tax.

Because of the continuing demand for back issues, all previous reports are available. Price: $6 each (for U.S., Canada, and Mexico), and $7 elsewhere; includes air mail postage.

Reduced rates are in effect for multiple subscriptions and for multiple copies of back issues. Please write for rates.

Subscription agency orders limited to single copy, one-, two-, and three-year subscriptions only.

Send your order and check to:
EDP ANALYZER
Subscription Office
925 Anza Avenue
Vista, California 92083
Phone: (714) 724-3233

Send editorial correspondence to:
EDP ANALYZER
Editorial Office
925 Anza Avenue
Vista, California 92083
Phone: (714) 724-5900

Name_____

Company_____

Address_____

City, State, ZIP Code_____