Information Systems Auditing

September 26-28, 1983
Milan, Italy

Earl M. Wysong Jr. and Ivo de Lotto,
Editors

North-Holland

INFORMATION SYSTEMS AUDITING

Proceedings of the International Conference on
Information Systems Auditing (ICISA)
September 26 - 29, 1983, Milan, Italy

edited by [illegible]

Earl M. Wysong, Jr.

Loyola College in Maryland
Baltimore, U.S.A.

and

Ivo de Lotto

Pavia University and CILEA
Italy

N·H
P C

1983

NORTH-HOLLAND – AMSTERDAM · NEW YORK · OXFORD

ISBN: 0 444 86778 3

Publishers:

Elsevier Science Publishers B.V.
P.O. Box 1991
1000 BZ Amsterdam
The Netherlands

Sole distributors for the U.S.A. and Canada:

Elsevier Science Publishing Company, Inc.
52 Vanderbilt Avenue
New York, N.Y. 10017
U.S.A.

Library of Congress Cataloging in Publication Data

International Conference on Information Systems Auditing
(1983 : Milan, Italy)
Information systems auditing.

"Organized by Application Software Development Center of CILEA ... sponsored by Sperry Univac, Italy"--P. ii.
1. Electronic data processing departments--Auditing.
I. Wysong, Earl M., 1925- . II. De Lotto, Ivo.
III. Application Software Development Center (Consorzio inter-universitario lombardo per l'elaborazione automatica) IV. Sperry Univac, Italy. V. Title.
HF5548.35.I56 1983 657'.453 83-16406
ISBN 0-444-86778-3 (Elsevier Sci. Pub. Co.)

PRINTED IN THE NETHERLANDS

INFORMATION SYSTEMS AUDITING
Earl M. Wysong, Jr. and Ivo de Lotto (eds.)
Elsevier Science Publishers B.V. (North-Holland)
©CILEA, 1983

INTRODUCTION TO INFORMATION SYSTEMS AUDITING

Dr. Earl M. Wysong, Jr.

ICISA Program Committee Co-Chairman
Professor of Accounting
Loyola College in Maryland, USA

The theme of this International Conference on Information Systems Auditing very well could be "Controlling Where Technology Is Taking Us." The computer often is the driving force in both business and government today.

The era in which we are living has been called the "information age" and well it should be. With advanced technology that is available today, we are seeing the merger of the formerly separate technologies of data processing, word processing, image processing and communications into an integrated philosophy. The information age promises to make us all more productive and to provide better bases for decision making.

Financial managers are relying more and more on information produced by computers. Just as an example of only one facet of the information age, consider the rise of the personal computer. The microprocessor was not even invented until 1975. Today every manager in an organization has the potential to have on his/her desktop more computing power than an IBM 360. Managers can access every other computer through a simple telephone connection and select all the information needed for decision making. They may then analyze it, graph it, word process it, and play "what if" games. Electronic mail, teleconferencing and telecommuting are current realities which are changing drastically the way organizations function.

With this increasing reliance by managers on computer-generated information, it becomes imperative that the information be accurate, pertinent, timely, and secure. Ah, there is the rub! Our challenge as auditors in the EDP environment is to control where technology is taking us and to see that systems are built to take advantage of the potential benefits of the technology while also improving the traditional internal controls to make the systems reliable and secure. The conference on information systems auditing was put together with four basic issues for consideration:

-- identify computer control weaknesses that are generally common to organizations,
— identify specific EDP control issues of today,
-- describe the application of traditional audit and control concepts to the new technology, and
-- define the responsibilities of managers and auditors in developing and maintaining control systems.

As you can see from the above discussion, the challenge of the program committee was to meld together topics and speakers to accomplish these objectives. We believe that we brought together some of the most notable and knowledgeable people on the selected topics in the world. We provided an appropriate mix of experts from both academia and the business world. Professors who have done extensive research and consulting to business and government were invited as well as professional consultants and practitioners with extensive business experience.

It is a natural beginning for the conference that the first paper presented examines several risks that concern managers and identifies some policies, procedures and practices to deal with these risks. The paper, entitled "Executive Management's Perspective on Information Systems Control," was prepared by Professors Alan G. Merten and Dennis G. Severance of the University of Michigan's Graduate School of Business Administration. This paper is the result of two research studies in which the authors participated.

The next paper is by William C. Mair, a partner of the accounting firm Touche, Ross and Co. This paper is entitled "Structure of Control Relationships" and describes how the complex relationships among various internal control classifications can be organized into a matrix that permits a model to be structured for forecasting the efficacy of a system's network of internal control.

This author's paper discusses the subject of auditor participation in systems design. The paper, entitled "Information System Project and Development Auditing: The Participatory Approach," provides the background for auditor participation and explains the "participatory approach." Further, the paper explains specifically how the auditor should participate in each phase of the system design life cycle. The author is a professor with Loyola College in Maryland and is also affiliated with two of the cosponsors of this conference: the Association for Systems Management as a member of the International Board of Directors and the Association of Government Accountants as a member of the Editorial Board for its publication, The Government Accountants Journal.

Remaining with the same general theme, a paper by Claudio Ciborra and Giampio Bracchi of the Politecnico di Milano follows. The paper, entitled "Systems Development and Auditing in Turbulent Contexts: Towards a New Participative Approach," compares and contrasts the participatory approach with the more traditional approaches. The paper is based upon a field study dealing with systems development projects in Norway.

The next paper deals with a very critical area of the EDP environment, "Control Activities in Database Management." It is co-authored by P. Gargiulo and G. Caldiera of Italsiel, Rome.

Thomas E. Bell of the Computer Technology Group, is the author of the next paper on "Auditing Data Processing Cost Allocation." This paper presents an audit approach to evaluating a cost allocation system by following the flow of costs through the system.

George J. Febish of Febish Associates follows with a paper, entitled "Cost Analysis: A Management Viewpoint." The paper provides a methodology for identifying both the cost and the value of information as a basis for managing the "information factory."

A paper by R. Claudio Miano and Marco Dori of the accounting firm Arthur Young & Company is presented next. This paper, entitled "Application Software Reliability Evaluation," provides a very interesting discussion on a new auditor specialization for evaluating software packages in the marketplace and issuing an audit opinion as to their reliability.

Next, Gianmario Castelli of Reconta Touche & Ross of Milan further discusses the subject of auditor participation in the systems development process. His paper is entitled, "The Role of the EDP Auditor in the EDP Systems Design and Development." The author is also president of the Italy Chapter of the EDP Auditors Association, which is one of the cosponsors of this conference.

A paper entitled, "A Flexible Metrics for Software Auditing Activities," is a natural follow-on to Castelli's paper. This paper is authored by Saverio Soccorsi Aliforni and Carolina Matarazzi of Italsiel in Rome.

Piercarlo Maggiolini of the Universita della Calabria presents a paper dealing with an "Economic Assessment of Information Systems and the Effectiveness/Efficiency of Computer Technology. In this paper the subject of the application of cost/benefit analysis is discussed in the context of information systems. It discusses also the economic evaluations of information systems through the application of marginal analysis of micro-economic theory.

Professors Gordon B. Davis of the University of Minnesota and Ron Weber of the University of Queensland, Australia present a paper on "Auditing Advanced EDP Systems: A System Change Model," The paper is based on concepts from systems theory and the results of research by the authors of internal EDP auditors on an international level.

The paper by Michael F. Morris of Management Advisory Services presents an insight to an area where auditors have feared to tread, but can be very important if auditors are to provide the best service to management. "Auditing Benchmarks Used in Information System Procurements" discusses the auditor's tasks in preparing for benchmarking, performing testing, and validating software and hardware performance.

The next presentation, entitled "Audit Language Design and Implementation" is authored by Booth, Longstaffe, Trowsdale and Will, all professors of the University of Victoria, Canada. This paper is the result of research conducted in Germany in the summer of 1983.

The paper presented next is by Linda J. Bellerby and deals with the modern EDP environment. The paper, entitled "Guiding Audit Activities through the Turbulent EDP Environment," discusses how the components of EDP activities and their interdependencies can be used to focus the audit on the areas of concern that will be the most useful to management.

The paper by Edward H. Murray of Management Advisory Services recognizes the newest challenge for auditors. It is entitled "Audit Management Perspectives: An Integrated Approach to Microcomputer Audits" and provides information on how auditors can approach this difficult area.

The final paper of these proceedings is presented by J. J. A. Leenaars of Moret & Limperg of Eindhoven, The Netherlands. The paper is entitled "A Computer Centre Audit." It defines five specific investigation objectives which must be part of a computer center audit and two others which are optional.

The final formal activity of the conference is a panel of experts to answer questions regarding "Cost-Benefit of EDP Auditing." The panel consists of the invited speakers to this conference and is chaired by Professor Davis. Each of the panel members provide a short presentation on the subject. This panel discussion is a most fitting conclusion to the conference.

Finally, my colleague and co-chairman of the program committee, Ivo De Lotto, provides the concluding remarks. Professor De Lotto is associated with Cilea in Milan and deserves a great deal of credit for his efforts in putting together this conference.

As I mentioned before, this International Conference on Information Systems Auditing brings together some of the foremost experts in the EDP auditing environment. The subjects presented by these authors are timely and pertinent. Some of the subjects present an innovative approach and some may be provocative. In any case, the material presented here will be of value to all of you and will provide a basis for your career enhancement.

TABLE OF CONTENTS

PANEL DISCUSSION: COST – BENEFIT OF EDP AUDITING

INFORMATION SYSTEMS AUDITING
Earl M. Wysong, Jr. and Ivo de Lotto (eds.)
Elsevier Science Publishers B.V. (North-Holland)
©CILEA, 1983

EXECUTIVE MANAGEMENT'S PERSPECTIVE ON INFORMATION SYSTEMS CONTROL

Alan G. Merten and Dennis G. Severance

Graduate School of Business Administration
University of Michigan
Ann Arbor, Michigan 48109
U.S.A.

INTRODUCTION

Many senior executives view computer and information technology as both the potential basis for management control systems which can reduce both business risk and internal risk and as a major potential source of internal control risk. Often, this "schizophrenic" attitude toward the technology grows worse as the technology is more widely used within the organization and as it is physically dispersed throughout the organization.

When senior and functional executives were recently asked[1, 2] to identify the role of computer systems in the management control process, they identified the following four categories:

(1) an aid in analysis--forecasting, simulation, financial analysis techniques;

(2) record keeping and data processing for reporting purposesfinancial operating, activity, budget, project reports;

(3) performance of operational activities--billing, purchasing, accounts payable and receivable, payroll;

(4) operational control--inventory, order and work flow tracking, automated production processes.

On the other hand, when chief operating and financial executives were asked to identify their major source of control concerns they almost always included computer system failure and computer abuse.

The purpose of this paper is to 1) examine several exposures and false comforts that concern informed executive managers and 2) to identify some policies, procedures, and practices that are being used in well-managed companies to deal with a variety of management control issues related to computer and information technology.

Most of the findings presented in this paper resulted from the previously referenced two research studies funded by the Research Foundation of the Financial Executives Institute in the United States. In total, over 450 senior managers from approximately sixty organizations were interviewed.

REAL EXPOSURES AND FALSE COMFORTS

The risk of a data processing disaster in American corporations today is significantly greater than realized by many senior level managements. Moreover, a number of ongoing developments in the information systems area are likely to further unbalance the current situation to the point where several spectacular catastrophies can be expected to bring the seriousness of the predicament into sharp perspective in the next few years.

Symptoms of A Problem

Corporate executives assess the situation as follows:

1. The demand for data processing services by user organizations continues to outstrip the supply of professionals qualified to deliver these services.

2. Technological improvements in the computer hardware and communication industries will continue to provide increased capabilities at reduced prices, and thus further fuel the demand for data processing services.

3. Users are more concerned with defining the functional services they require than they are with designing failsafe controls for inclusion in those systems.

4. The success of a data processing staff is most often measured in terms of its ability to respond quickly to user needs.

5. The combined development, documentation, and operating cost of tightly controlled data processing systems are sometimes an order of magnitude greater than the cost of an undercontrolled system. This cost will grow larger as we move more deeply into an era of distributed, online data processing systems.

6. Data processing professionals are often not trained in nor motivated by the need to control computer system access. On the contrary, they view their primary role as providing ease and speed of access.

7. There are no industry standards to define the nature or the scope of adequate EDP controls.

8. There is virtually no sharing of control concerns, control experiences, and control methods among corporations.

9. Corporate managements often believe that their data processing operations are much more tightly controlled than do either the heads of internal audit or the managers of data processing.

10. The effort required to certify the adequacy of controls on every existing data processing system is far beyond their ability, given current expertise and manpower.

11. Many existing control systems are inadequate to defend against subversion by even individual data processing professionals.

12. It is generally impossible to anticipate the full impact of a particular loss, and the probability of any single disaster appears to be extremely small. There is a natural tendency to underestimate these factors, and thus to build systems which are undercontrolled.

13. The demand for data processing professionals is very high. While potential corporate loss in the event of a data processing disaster is very large, the risk to the individual "responsible" for the loss is very small.

In combination these facts suggest that computerized systems in many organizations may be undercontrolled. There are several reasons to explain why this problem may go unrecognized.

Placeboes and False Comforts

We observe that circumstances and conditions are present in many companies today which will bias a rational manager to build and operate computerized systems which are in fact undercontrolled. The feedback systems upon which management relies for warnings of impending problems are delivering signals which might easily be misinterpreted. Specifically, we believe that there are four sources from which executives derive false comfort when evaluating the adequacy of their data processing control system.

First False Comfort: "To my knowledge there has never been a significant, EDP-related loss of control in this company. Moreover, it is rare that I hear of such a case in any company."

There are two issues to consider here. How well is management informed of past events; how good an indicator of the future is the past? Near-disasters are relatively common: the inexperienced operator who destroyed two backup copies of a master file while attempting to restore the original; the psychotic employee who succeeded in shutting down a corporate data center 56 times in a 24-month period before detection; a sudden realization that secret product formulae were stored without protection on the computers of an outside service bureau; the 500 million characters of online data destroyed when dirt was fed accidentally into a ventilation system.

In situations where significant losses do not occur, there is really no reason to trouble upper management with the details of a situation which is being corrected. When an operational disturbance is noticeable, the simplified explanation of "hardware problems" is easily understood, readily accepted and carries no professional stigma.

There is virtually no sharing of control concerns and experiences within the data processing community. There is little natural forum for such an interchange, and there is, moreover, an inherent aversion to revealing embarrassing facts in public.

Our ability to conceive and build useful computer systems appears to far exceed our ability to imagine possible misuses and abuses of those systems. Many of the controls installed in financial systems today were devised only after a significant loss painfully demonstrated a need. Having suffered a defalcation, companies are reluctant to report it for fear that bad publicity will lead to a loss of public confidence and potentially to a monetary loss greater than the crime itself. In instances where a loss results from incompetence rather than embezzlement, there is even less incentive to reveal it.

The net result of these facts is that past instances of computer related losses are likely to be greater than management realizes. More importantly there is evidence to suggest that things will get worse before they get better. Recent breakthroughs in computer and data communication technology will soon make it economically feasible to distribute computer processing capabilities widely throughout an organization, and simultaneously make it inexpensive to provide access to large volumes of data from geographically remote locations. Unfortunately, control procedures to regulate such access adequately are still evolving, and from evidence to date, the necessary mechanisms are likely to be quite complex and very expensive. To satisfy demand for service rapidly and with minimum cost, there will be great temptation to install systems with unproven controls.

Second False Comfort: "Neither our internal auditors nor our external auditors have reported any major weakness in our data processing controls in the past five years."

In general, data processing managers believed that the internal and external auditors combined did not possess sufficient expertise or manpower to certify the adequacy of controls in existing systems. Neither could they believe the auditors were able to detect circumvention of these controls, assuming that the controls were originally installed. Even in those ortganizations where auditor quality and involvement are highly rated, the general feeling is that the situation is improving, not that existing systems are adequately controlled.

The fact that such a situation might exist without management knowledge should not be surprising. Any professional is reluctant to raise problems for which an acceptable solution cannot also be offered. There are few proven or accepted control standards to be cited by these professionals, and the cost associated with control practices which do exist are very high. Moreover, many control procedures are organizationally unpopular, while the probability of a detectable loss in many exposure areas is low. It is easy to imagine a tendency to rationalize either that a particular situation is actually not a significant problem or that it will not lead to a "material" loss.

Third False Comfort: "Our security systems are the best that money can buy. Because I realize that sound computer system control is essential to this company, I have approved every control expenditure which has been recommended to me."

A computer control system is as strong as its weakest link. In many organizations, some facets of control are handled with great attention to detail and at substantial expense, while others are completely ignored. One computer system room boasts the latest in computer controlled badge readers, while access to its databanks via local terminals is effectively unmonitored. A second system runs a database management system which controlled database access all the way down to the level of individual data items, while a backup copy of the entire database is kept in an unsecured tape library.

A widely publicized example of uneven controls involved the U.S. Social Security Administration. Shortly after spending $500,000 to install a new security system for its computer operations, unauthorized congressional investigators walked out of the computer complex with a set of computer tapes containing the names and addresses of 1.14 million beneficiaries. These files were the input for a system which generates $80 billion a year in benefit checks, and alteration of the file could result in a massive fraud.

Large control expenditures alone therefore do not assure adequate computer system security. A complete, and thoroughly analyzed, security plan is necessary for adequate control.

Fourth False Comfort: "The data processing manager of this corporation is a competent professional. By every standard that I have set, he has been successful in finally turning data processing in this organization around. I trust his judgment."

It is the plight of the data processing manager that gives greatest plausibility to the theory that computer systems are undercontrolled. Within most organizations, data processing is viewed primarily as a service function--it supports the collection, transmission, storage, retrieval, and display of information required by the other functional areas of the business. Users of data processing services are principally concerned with access to desired information; understandably, they seek quick, inexpensive development of efficient, easy-to-use systems.

The poor esteem in which some data processing groups are held today results precisely from their inability to meet this expectation of prompt service, economy, and simplicity. Data processing is traditionally criticized for long lead time on new system development (e.g., two years or more) and for projects delivered both late and over budget. It is on the basis of his ability to overcome this problem that many data processing managers are evaluated. Seldom are they critized about undercontrol.

Unfortunately, strong control is the antithesis of fast, inexpensive access. The analysis, design, and testing of new systems requires more time and uses more professional staff; the resulting system is generally less convenient to use and is always more expensive to operate. As with safety devices on automobiles, control mechanisms in computer systems provide no perceived functional benefit. They are not "needed" as long as the system continues to operate "normally," and this is exactly how the user expects that it will operate.

The conclusion is unavoidable that data processing managers must tend to underestimate both the probability of a control loss and the magnitude of its consequences in an environment which can be described as follows:

> "Users consider the audit trails to be nonsense."
> "The use of that control would probably triple the operating cost of this system."
> "Controls just do not interest EDP personnel."
> "If I forced my staff to comply with everything in those standards manuals, they would quit tomorrow."
> "Since no system can be totally controlled, how do I know how much is enough?"
> "How do you assign value to data center recovery in two days as opposed to two weeks?"
> "I am evaluated primarily on my ability to get new systems up quickly."
> "The internal auditors cannot detect the lack of controls or the circumvention of existing controls."
> "It is not clear that I am responsible for a loss of control in that system. It was built to user specifications and reviewed by internal audit."
> "The possibility of that loss is extremely remote."
> "If I were forced to leave this job, I would have little trouble in finding another."

PRACTICAL SOLUTIONS TO PERCEIVED PROBLEMS

Companies are continually seeking to find ways to improve their computer-based systems and to maintain adequate control over them. We found a considerable variety of solutions to perceived computer control problems and often a variety of solutions to the same problem.

1. Assignment of Responsibilities Among Concerned Parties.

Almost without exception, those we talked to in our interviews agreed on the importance of assigning responsibilities to the several participants, but in many companies this matter has not been fully and realistically resolved because it is very complex--much more complex than it at first appears to be. It necessarily involves the users of information systems services, that is, the operating department heads who rely upon the information produced by computer operations and who also request new systems as they appear needed. Of course it involves the information systems people also, both the management of that function and the various levels of technicians within it. Internal auditing, senior management, and possibly computer vendors and independent auditors also have at least an indirect relationship to the most effective use of computer based systems.

There seems to be agreement that specific statements of responsibility are desirable. Each of these participants should know what others expect of him so that he can correct those expectations if erroneous. Each participant also needs to know what he can expect of others.

In those companies which appear to have thought out the relationships and responsibilities involved, they seem to work out something like this: Line managers, the users of the information systems services, have the ultimate responsibility for the integrity of their data at all times, and for the accuracy and propriety of data processing. This is a responsibility they cannot shift to information systems. It is up to the users to determine the importance of their data and to satisfy themselves that it is entered, processed, and reported accurately, and that adequate backup plans in the event of catastrophe have been made. They also have the ultimate responsibility for the security of the data they supply. If they are not confident that information systems can satisfactorily meet their needs, they should not entrust their data to that department until appropriate safeguards are provided.

The users also have the final responsibility for the identification of needs and opportunities, and the potential for innovative applications. Of course, the capacity to meet those needs and opportunities must be provided to them by the information systems people, and the users can seek counsel from various experts in determining what opportunities exist. If data supplied or required by users should be classified into various levels of confidentiality, integrity, and recoverability, this also is a responsibility of the user.

If this seems to put a great deal of responsibility upon the user of information systems, and it does, the response is that there is no real alternative. If any of these responsibilities and rights are taken away from line management, that management loses some control of its function. Line management must have the final right to decide all these matters, and therefore it must take the responsibility for their proper resolution.

Information Systems

Information systems provides a service capability for the rest of the company. In doing so, information systems should meet the needs described by the several users within the company. Information systems also provides an education and consultation service to users, to senior management, and to internal auditors as these parties need help with technical problems.

In providing an adequate service capability to the several users within the company, information systems personnel should discuss with them their needs for systems development, for operations, and for security, and should be prepared to provide such services on a competitive basis. That is, if the users have access to equal or better services at less cost on the outside, or by doing it themselves taking all costs and benefits into account, the user should have the ability to take advantage of the situation.

Note that it is not enough for information systems to offer those services, it has to find a way to communicate its ability to serve the various potential users within the company. Thus, all its several services should be accurately described in terms that are meaningful to those who may have use for them.

Internal Auditors

We found a strong agreement that internal audit is responsible for confirming the inclusion of adequate controls within systems. That is, internal audit is widely perceived as the function which should assure that adequate controls are designed for and programmed into new systems by some "quality assurance" group located either in internal audit or information systems. This means that the internal audit department must participate as early as possible in the design of the system so that necessary controls are present in the initial system rather than added later. System modification is almost always costly and may not be effective.

To some internal auditors, this raises an important question. If the quality assurance group is a part of internal audit, does participation in system design infringe upon necessary audit independence? Because any audit opinion is only as useful as the real and perceived independence of the auditor, those who practice auditing have come to have great concern for their independence. Many internal auditors are troubled by any assignment which they feel conflicts in any way with their independence. Others accept the fact that the contribution to the company in participating as a consultant in the design and inclusion of adequate control measures for new systems more than balances any possible loss to the company of internal audit independence.

If internal auditors are to participate in the design of computer based systems, they must have significant knowledge of computer systems. As yet, this is a relatively rare talent or expertise for internal auditors to possess. One of the ongoing activities we saw over and over again was the effort to combine audit expertise with some degree of computer expertise, resulting in what is often referred to as an "EDP auditor."

Senior Management

Senior management is responsible for the ultimate success or failure of the company. To that extent it has some responsibility for everything that happens within the company. This responsibility is discharged through a system of management control composed of: 1) the control environment, including stated goals and policies; 2) a process of opportunity and risk analysis to determine what actions the company should take; 3) the selection and application of control procedures to meet those opportunities and risks; and 4) monitoring of the procedures both with respect to their effective application and their overall sufficiency. Any breakdown of management control over computer based systems reflects to some extent upon senior management's success in performing its responsibilities.

Computer Vendors

In assessing the responsibilities which computer vendors bear, one must make a distinction between legal responsibility and those obligations which are effectively forced upon the vendor by competition. We think it is not an unfair generalization to say that most vendors wish to accept the minimum legal responsibility possible. This is not at all unreasonable. When computer resources, whether hardware or software, are sold or leased to a given company, they pass out of the hands of the vendor who then has no control whatsoever regarding their use or misuse. In our litigious society, business failure of any kind seems to result in charges against anyone remotely connected with the company. To protect themselves against otherwise possibly catastrophic charges, computer vendors define their commitments very precisely by contract. That commitment covers the quality of their product, clear and accurate specification of its performance capabilities, and effective training in its use. They can promise no less and dare promise no more.

In contrast to the legal liability restricted by contract, vendors have a great desire to save their customers' viability and will do anything within reason to help a customer recover from any kind of computer disaster. In addition, competition is a strong incentive to providing such services. If a competing vendor is able to suggest that its emergency services, although not required under the contract, are far better than the emergency services offered by other computer vendors, it has made a useful marketing point.

Independent Accountants

Independent accountants offer computer-related services in two ways. First, in connection with the annual audit, they review the company's internal accounting control and adjust their audit programs accordingly. In addition, many of them have a management services department which in some cases offers consultation on a variety of computer-based problems. As auditors, independent accountants do indeed review internal accounting control, but this is a very limited review, carefully defined in the audit literature, that has as its purpose only the determination of the appropriate extent of audit procedures to be followed. If in the course of that audit review the auditors find a basis for making suggestions to the client company, they will do so, but that is a by-product rather than the primary purpose of their review. A review of management control systems in the sense that would be necessary if the auditor were giving an opinion as to the quality of that control system must be contracted for as a separate engagement and would go beyond the review made for audit purposes only.

2. Assimilation of Information Systems Activities and Personnel

We became strongly persuaded that those companies which had the greatest success in maintaining control over data processing and the whole field of information systems were those which had done the best job of assimilating information systems into the total organization. Any step that increases mutual understanding between information systems professionals and the other members of the business organization, anything that facilitates communication or builds loyality to the company, any measures that help all concerned make their best contribution to the corporation's success should at least be considered. Without the feeling that they are part of the company, it seems unlikely that many members of the information systems function will be able to serve as well and contribute as much as they would knowing that they were fully accepted by other members of the organization with the same opportunities and rewards for effective service.

A step taken to make information systems an integral part of the company is to obtain user involvement at the highest possible level. Operating managers need to know and understand computer potentials, limitations, and costs if they are to make the most effective use of computer facilities. Given the variety and significance of other demands for their attention, obtaining this kind of knowledge is likely to be very slow unless special efforts are made in some kind of formal or semi-formal training programs.

General staff training in data processing for members of the company's organization who are not familiar with information systems is not common as yet but seems to be growing. In addition, there are efforts to intermingle information systems and non-information systems personnel on team projects and to transfer people back and forth from one department to another, for example, from information systems to operations and then back to information systems, or from internal auditing to information systems and back to internal auditing. All of these steps aid in reducing the barriers which so often exist between information systems personnel and the rest of the company.

3. Assuring Reliable Computer Security

We found continuing concern as well as considerable activity with all aspects of computer security. This includes the physical security of the staff, machines, and data, the reliability of the computer operation, and the integrity of data. Included is a wide variety of measures and activities.

Creation of Appropriate Control Attitude and Environment

A number of incentives have encouraged some companies to undertake a corporate-wide program to improve information security and control. In some cases, it is a recognition that the combination of exposure and the importance of data and systems requires attention. In other cases, it is the knowledge of reported cases in similar companies. One approach is to establish a corporate information security task force to review the company's procedures and to make recommendations. A number of companies use what they call a security control committee which often involves other risk conscious groups such as insurance and security in the development of company policies.

Most of the executives we talked to on this issue mentioned increased attention in staff training programs to adequate control and protection of corporate data. A common practice is to establish for each major systems project a control and review group. This group is assigned to assure that in the design of the system, provision is made for adequate control measures. Before the system is turned over to the operating personnel, some quality control group would determine whether satisfactory control measures were in place and working. Some companies have managers of systems integrity whose principal task is to assure that control measures are provided for, serving satisfactorily, and adequately monitored.

A number of executives reported that their company's corporate audit committee takes an active role in reviewing computer control and security procedures, thereby strengthening both the system and the environment in which it operates. In such cases it is common to include security in the mission statement for the information systems function. Other companies fix the responsibility for computer site administration in a specific officer who thereby becomes, in effect, something of a computer security executive.

Companies were advised by some executives we interviewed to purchase hardware and software systems with built-in controls wherever possible, and to discuss with the vendor in advance the nature and extent of those controls as well as the company's need for them.

Development of Contingency Planning

In the experience of almost any company which employs computer-based systems extensively, there comes a point at which it recognizes the extent of its computer dependency and then begins to think in terms of responding to various contingencies. The response runs all the way from providing complete backup systems at another site to disaster plans with named disaster team members and established procedures. The computer vendors we interviewed believe it is useful for a company to have people named to give consideration to possible risks and to how they would respond should a risk be realized, especially if the company is unable to develop a complete backup system. Testing backup systems and disaster plans is also highly desirable if for no other reason than to know that—they exist more than just on paper. One experienced executive said, "An untested plan is no plan at all."

Involvement of Auditors

Concern with computer security seems to direct the attention of executives almost unavoidably to make use of the talents and abilities of the company's internal audit staff. In a number of cases, attempts to utilize that audit staff resulted in efforts to improve and strengthen its capacity to deal with computer-based systems. In some cases, personnel were transferred from the information systems department to internal auditing, or EDP expertise and systems competence were sought on the outside in order to provide the more