Division of Research
Graduate School of Business Administration
The University of Michigan

July 1980

DATA PROCESSING CONTROL: A STATE-OF-THE-ART SURVEY OF ATTITUDES AND CONCERNS OF DP EXECUTIVES

Working Paper No. 224

Alan G. Merten
Dennis G. Severance

The University of Michigan

Data Processing Control: A State-of-the-Art Survey of Attitudes and Concerns of DP Executives

Alan G. Merten and Dennis G. Severance

Computerization has become essential to the effective management of large organizations. This new corporate dependency upon computer availability, the associated concentration of valuable and sensitive data into computer memories, and the placement of critical responsibilities into the hands of technically oriented data processing personnel have given rise to new forms of corporate risk and a potential for serious control problems. Our recent study of EDP control in U.S. corporations was undertaken with five questions in mind:

- Has reliance on computer services become so important in business activity for some companies that denial of computer services could be catastrophic in terms of continued operations?
- Have appropriate steps been taken to provide a satisfactory alternative in the event of computer breakdown to avoid either catastrophe or significant cost?
- Is the internal audit function technologically competent (1) to participate in the development of new electronic data processing systems to the extent necessary to assure that adequate controls are provided, and does it actually do so; and (2) to monitor such programs once they are implemented?
- Does the utilization of distributed processing and database technology subject the company's accounting and/or other data to undue risk of unauthorized access and manipulation?
- Has electronic data processing technology outrun management's ability to provide "reasonable assurance" that personnel failure will not occur?

1. Background for the Study

In the spring of 1979 under the auspices of the Financial Executives Institute (FEI), we and five other faculty members from the Graduate School of Business at The University of Michigan undertook a study of the state of the art of internal control in U.S. corporations. A variety of prior evidence suggested that the control aspects of data processing were a source of concern to management, and our information systems background was viewed as an important complement to the expertise of colleagues in accounting, finance, law, and organizational behavior. In total, the projects extended over a period of eighteen months at a cost of more than $250,000.

The impetus for the study arose with the passage of the Foreign Corrupt Practices Act of 1977 (FCPA). The Act was essentially a congressional response to a series of highly publicized incidents of malfeasance by a small but significant number of U.S. companies. These included Lockheed's payments to Japanese officials in connection with efforts to sell the L-1011, and ITT and Gulf Oil's political payments in a number of countries. In addition, Watergate findings revealed that a number of publicly-owned companies were engaging in a wide variety of illegal or questionable practices. The Security and Exchange Commission (SEC) was alarmed to note that some companies had falsified entries related to these activities in their financial records.

As enacted by Congress, the law contains both bribery provisions defining stiff penalties for a variety of illegal payments and accounting provisions which preclude executives from pleading innocence by virtue of ignorance of such payments. In short, the bribery provisions make illegal any direct payments to foreign officials, governments, agencies of governments, political parties, or candidates for office, if the payments are intended to influence the recipient party to assist in obtaining, retaining, or directing business. The accounting standards provisions require that a corporation establish and maintain an

"adequate" system of "internal accounting controls" and specifies penalties of personal fines and imprisonment for violations by executives. Sound business practices had become law.

Ambiguities in the wording of the Act caused concern in the business community. It was feared that the SEC, to enhance its power, might interpret the law broadly and use it selectively as a weapon in forcing consent decrees in actions brought on other grounds. The Michigan study was designed to document the state of the art of internal control in U.S. corporations with particular emphasis upon identifying common control concerns and standard control practices. Potentially, such a profile would have value to a corporation first as a benchmark for analyzing and evaluating its control system, and subsequently as a de facto standard against which the reasonableness of the system might be argued in legal proceedings.

Data for our control assessment was drawn from both a widely distributed questionnaire and personal interviews with more than 350 corporate executives. The questionnaire consisted of approximately 250 items of inquiry and required approximately four to six hours to complete. It was distributed to the chief financial officers of the Fortune 1,000 and an additional 1,000 company members of FEI. The questionnaire was completed by 673 firms representing a broad cross section of industry types and company sizes (see Table 1).

Structured interviews with corporate executives complemented our questionnaire data. A one day visit by two team members was conducted at 50 U.S. corporations randomly selected from the Fortune 1,300. Interviews followed a set of pilot-tested guides and in general were conducted with the chief financial officer, controller, legal counsel, internal auditor, senior information systems officer and various staff and operating executives. Table 2 contains a description of the interviewed companies.

Table 1

Classification of Firms Responding to Mail Questionnaire by Industry Classification[1]

Industry Category	Category	SIC	Number of Companies	%
1	Agriculture	01-17	46	7.3
2	Manufacturing	20-39	404	64.2
3	Transportation	40-48	26	4.0
4	Utilities	49	27	4.3
5	Wholesale/Retail	50-59	42	6.7
6	Financial	60-67	52	8.3
7	Services	70-89	33	5.2

[1]Standard Industry Classification (SIC) numbers were assigned to each respondent for which information was available. The assignment was based on the description given by the respondent and other publicly available information on the company. While 673 questionnaires were returned, only 630 of the respondents provided sufficient information to determine the industry classification.

Table 2

Classification of Firms Interviewed by Industry Group

(Based on Industry Codings in the Fortune 1000)

Code		Companies Visited
20	Food	4
22	Textiles, vinyl, flooring	1
23	Apparel	1
26	Paper, fiber & wood products	1
27	Publishing, printing	2
28	Chemicals	4
29	Petroleum refining	3
32	Glass, concrete, abrasives, gypsum	2
33	Metal manufacturing	5
34	Metal products	1
36	Electronics, appliances	3
37	Shipbuilding, RR and transportation equipment	3
38	Measuring, scientific, photographic equipment	1
40	Motor vehicles	1
41	Aerospace	1
43	Soaps, cosmetics	1
45	Industrial and farm equipment	2
48	Broadcasting, motion picture production & distribution	1
	Total from Fortune 1000	37
	Life insurance	3
	Diversified financial	2
	Retailing	3
	Transportation	2
	Utilities	3
	Total	50

2. A Summary of Relevant Study Findings

This article will focus primarily upon issues of EDP control as seen through the eyes of data processing executives. A brief review of broader study conclusions and a summary of EDP concerns from other corporate vantage points provide a healthy perspective for those details as presented in Section 3. Several general conclusions of the study are relevant:

1. While most executives view control as an integral part of the management process and accept this responsibility, they consider the Foreign Corrupt Practices Act to be an unwarranted and blatant intrusion of big government into the affairs of private business.
2. The great diversity which exists in the character and risk profiles of U.S. corporations make it unlikely that detailed omnibus standards can be devised by which to judge the adequacy of control practices in specific companies.
3. Most executives believe that their company's present internal control systems constitute a rational balancing of risk and cost; that substantial additional money spent on control is not likely to be cost-beneficial.
4. Company executives by and large have no knowledge of internal control concerns and practices in other companies, even within their own industry.
5. The aspect of internal control that troubles executives most is their increasing dependency on computers for operational effectiveness and financial reporting.

The last point is perhaps the most interesting. In response to the question: "Which of your company's activities cause you the greatest concern from an internal control point of view?," 61.2% of our 673 questionnaires contained the

response, "electronic data processing." Volunteered comments in the margins of the questionnaires and our subsequent interviews reinforced the conclusion that corporate executives consider data processing control to be a major problem area.

Our interviews revealed that the concerns of financial executives often reflect a general uneasiness about the overall state of affairs in their data processing departments rather than specific fears of identifiable control losses. Corporate executives are aware of their organizations' increasing addiction to computers, both for operational control and for information purposes. Data processing budgets may claim as much as 3 percent of total sales, and are sometimes measured in hundreds of millions of dollars. Yet data processing departments are noted for high personnel turnover, budget overruns, tardiness in completing projects, and a chronic shortage of qualified personnel. Couple this with the widespread belief that computer technicians feel more allegiance to their technology than to the company that employs them, and the causes of management's uneasiness are clear.

We obtained more specific insights into the nature of the computer risks faced by corporations during our interviews with the chief internal auditors. They were concerned about both computer failure and computer abuse. On the one hand, many companies have come to rely so heavily on their computers for the daily processing of transactions and control of operations that a serious computer breakdown could lead to a substantial curtailment or stoppage of operations. This Achilles' heel of modern corporations has not gone unnoticed by radical groups in Europe, where numerous acts of sabotage against computer centers have occurred in recent years. Our study found that few U.S. corporations are adequately prepared to cope with such a contingency.

Computer abuse was the second concern of the auditors. To an ever increasing degree, sensitive corporate data, especially financial and accounting data, are stored in computer memories accessible from remote terminals. They are exposed to potential manipulation, misuse, or destruction through operations that require only a fraction of a second for completion and which can be initiated through terminals hundreds of miles away. Companies that are extremely cautious about cash control may quite unconsciously permit other employees to "get their hand in the till" indirectly through the initiation of transactions at data processing terminals.

Technological developments like mini- and microcomputers and distributed data base systems increase the availability of computers and computer terminals. Auditors suggest that predicted technological advances in the near future are likely to increase the internal control risks. They fear that our ability to conceive and build useful computer systems may far exceed our and their ability to imagine and guard against possible misuses, abuses, and potential attacks against EDP systems.

Many of the controls incorporated in financial systems today were devised only after a significant loss painfully demonstrated a need where none had been recognized previously. Auditors frankly admit that the time and effort needed to certify the adequacy of controls on every existing data processing system are far beyond their ability, given current expertise and manpower. They fear that to satisfy demand for service rapidly and with minimum cost, the data processing department will face strong pressures to install systems with unproven controls.

Interviews with heads of data processing departments detailed in Section 3 provide support for the auditors' fears. Within most companies, the data processing organization is viewed primarily as a service function - it collects, transmits, stores, retrieves, and displays information required by other

departments of the business. Those who call on the data processing department for service are principally concerned with the immediate availability of desired information. They seek quick, inexpensive, 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.

The fact is that strong control is the antithesis of fast, inexpensive access to information. The analysis, design, and testing of a well-controlled system require more time and more professional staff than an uncontrolled system. The controlled system is generally less convenient to use and is always more expensive to operate. Data processing professionals generally tend to feel that their role is to provide ease and speed of computer access at minimum cost. Seldom are they motivated by, or trained in the need for, internal controls.

This reflects the environment in which data processing professionals operate. There is little demand for control consciousness. No industry standards exist to define the nature or the scope of adequate control over data processing, and there is virtually no sharing of control concerns, experiences, and methods among corporations. New developments make the traditional system of checks and balances provided by accountants and auditors largely ineffective.

As we will see later, most data processing managers are critical of the technical competence of auditors. They believe auditors have neither expertise nor manpower sufficient to evaluate the adequacy of controls now included in existing systems. Nor do they credit auditors with the ability to detect circumvention of controls that do exist. To add to the seriousness of the situation, most data processing managers conceded that their own control systems are inadequate to defend against subversion by data processing staff members even without collusion.

With all this in the background, it is no wonder that financial executives have an uncomfortable feeling about their data processing systems. Even so, we conclude that, by and large, they believe it to be more tightly controlled than do either their chief internal auditors or the heads of their data processing departments. The specific concerns of data processing executives are described below.

3. Summary of DP Executive Interview Data

Our intent in each of the 50 corporations we visited was to interview the official responsible for all corporate data processing activities. This was not possible in some cases where the person in charge of data processing at the corporate headquarters had either no responsibility or only dotted line responsibility for data processing in the division or line units. In all cases, a structured interview was conducted with the senior official with responsibility for EDP at the corporate headquarters. The limited extent of electronic data processing in some of the companies interviewed was such that useful responses were obtained from fewer than 50 companies on some questions.

THE COST OF DATA PROCESSING

As a budget item, the cost of data processing varies greatly from company to company, but for most large corporations, it has become a significant item in total operating costs. Within the 50 companies interviewed, EDP staff size varied from 2 to 22,000, with an average of 384 people engaged in data processing.

The average data processing budget included $20,000,000 for computer hardware and software, and personnel costs with a range from $70,000 to $94,000,000. Personnel costs account for 55% of that total, on average.

Thirty-seven percent of the data processing managers queried find their present budgets inadequate, some significantly so. The remaining 63% consider

their budgets adequate, but sometimes with qualifications. Responses like the following were received:

- "I could use more organizational capacity, but I cannot control growth in that capacity at a faster rate."
- "Budget is adequate for what we agree to do."
- "Budget is adequate but not distributed properly."
- "We must learn to use our present budget more effectively."
- We are wasting money now."

If more resources were made available, the overwhelming majority of interviewees (70%) would use them for recruitment of new personnel and/or education of present staff members to support the existing demand for electronic data processing services. Availability of resources is always a constraint, but most managers find attracting and keeping competent electronic data processing professionals a problem even when resources are available. Another 27% of respondents would use any budget increase primarily for hardware and software development.

TYPES OF SYSTEM SOFTWARE

As expected, there exists great variation in system and application software. Major applications of electronic data processing range from 5 to 500 in a single company, with an average of about 80. To service these applications, the number of individual computer programs range from 70 to 20,000,with an average of 400.

COBOL is by far the most popular language; a full 80% of the programs are written in that language. The next most popular is some assembly level language. Although only about 28% of all the programs were described as interactive, several managers noted that the computer resources consumed by the interactive applications were much higher, close to the 80% mark.

The proportion of interviewees indicating availability of, and therefore probably some use of, specialized system software is presented in Table 3.

TABLE 3

PROPORTION OF FIFTY COMPANIES WITH VARIOUS FORMS OF SPECIALIZED SOFTWARE

Specialized Software	Percent of Companies
A database management system	84
A data dictionary	54
A teleprocessing monitor	70
A hardware or software monitor	46
Some special audit software	46

The average number of major data files stored by a company was thirty. The size of these files ranged from one-half million to three billion characters; the average number of stored characters was 50 million. The percentage of corporate data stored on tapes compared with other storage possibilities is shown in Table 4.

TABLE 4

DATA STORAGE ON TAPE

Percent of data stored on tape	Number of companies	Percent of companies
95% - 100%	7	21%
90% - 95%	4	12%
50% - 90%	10	31%
1% - 50%	9	27%
0	3	9%
	33	100%

Most corporations use their computers to collect and process data in support of several business functions. The extent of support may range from a single program to several systems of multiple programs. Electronic data processing managers were asked to assess the control sensitivity of various applications without regard to the current quality of their own EDP controls. The systems identified as posing the greatest degree of potential risk are listed in Table 5.

TABLE 5

Rank	Program(s)	Times Mentioned
1.	Accounts payable	15
2.	Payroll	12
3.	Accounts receivable	11
4.	Inventory	8
5.	Sales, order entry, credit, and billing	8
6.	Shareholder records	3
7.	Engineering and scientific data	3
8.	Financial management and forecasting	2

RESPONSIBILITY FOR INTERNAL CONTROL BREAKDOWNS

Data processing managers were asked to fix the blame if an internal control breakdown had actually occurred in one of the sensitive systems listed in Table 5. The responses vary and in total seem to suggest that at this stage in the development of relationships between the data processing function and the rest of the company, some important responsibilities have not been fixed as well as they might be. Forty-three responses were received, and are reported in Table 6.

TABLE 6

RESPONSIBILITY FOR CONTROL BREAKDOWN IN EDP PROGRAM(S)

Responsibility charged to	Number of responses
Data processing	18
User of data processing	14
Internal audit	1
Data processing and user	3
Data processing and internal audit	1
User and internal audit	1
Data processing, user, and internal audit	5
	43

Comments by the data processing managers emphasize the developmental or evolutionary state in which the internal control over data processing activities finds itself at this time:

- "If internal audit participates in the design or development of data processing programs, then they are responsible; if they do not participate, data processing is responsible."
- "The project leader is responsible - and he may come from the user group or from data processing."
- "As users become more involved in specifying the requirements for systems, they should share the responsibility."
- "The user is responsible, but users do not realize their responsibility."
- The user defines what should be in the system, data processing install what is specified, and internal audit reviews the specification as installed."
- "It has to be data processing since the user and internal audit do not understand electronic data processing systems."

INTERNAL CONTROL ASPECTS OF THE DATA PROCESSING FUNCTION

The introduction of computers into data processing on a large scale in any company impacts internal control in two ways. First, computer hardware, software, and the data and documentation which in total comprise the data processing system are themselves valuable assets to be "safeguarded", to use the FCPA language. Second, the computer's data processing systems and activities support and complement more traditional systems of control, and can be subverted to a variety of ends detrimental to the company. As a result, data processing groups must be seen as serving three roles within a company, each of which has internal control implications:

- functional responsibility for the management of the EDP assets;
- responsibility for the integrity and satisfactory operation of existing computerized systems; and
- responsibility for the design and implementation of new computerized systems.

Functional Management

Management of data processing assets does not appear to offer unusual internal control problems to any greater extent than does the management of other valuable equipment. In our discussions with data processing managers, they frequently made reference to operational control strategies based on such popular concepts as overhead charge-back, management by objectives, chief programmer teams, structured programming, database management systems, prototype development systems, and hardware and software monitoring systems. Such practices were considered to be quite valuable in increasing the effectiveness of data processing operations.

Operational Security.

Three aspects of operational security were covered in the interviews :

- control over physical access to the data processing facilities;
- control over access through the computer to stored programs and data; and
- computer facility backup in case of physical disaster or computer failure.

Nearly one third of the organizations visited had no special control over access to the data processing area of the building. They rely on normal security precautions only, and assume that a receptionist and employee badges provide the necessary protection.

In the majority of the companies, some additional combination of locking systems, guards, and television surveillance is employed. Thirteen percent of these companies described protection strategies based on "rings of security" within the data processing center devised to provide increased security for critical hardware and valuable or sensitive data. Only 8 percent of the centers were described as "closed shops" which would grant entrance only to authorized computer operations personnel.

Access to data through the computer is another matter. A person could do great damage to computer facilities if access to the computer could be gained. To influence or access the computer programs or data requires some degree of computer expertise. Through a system of user identification and passwords comparison, the computer's operating system can identify authorized users and verify their right to execute specific programs and to access requested data. Approximately one eighth of the companies visited do not take advantage of this possibility.

Of those utilizing some kind of password protection, 75 percent use it only to control entry to the system. Once one has the password to get into the system, that person has access to everything within the system. Password protection to restrict access to individual files was reported to be utilized only rarely.

Many managers described exploratory use of a database management system which could provide "data locking" down to the level of specific data items, but not many of these are yet in actual use. Several data processing managers hold that the computer operator can play a key role in controlling access to the computer system merely by visually identifying all those who seek to use it, by examining requests for the opening of data files, and by calling back to authorized telephone numbers when remote access to the computer system is requested.

A majority of the managers interviewed acknowledge that they view rapid recovery of EDP operations following a physical disaster, or any other event depriving them of the use of their computer, to be an important problem. To some extent this sensitivity is the result of recent prodding by external auditors. The interview guide requested a description of the company's formal plan for coping with a loss of computer capability. The responses are noted in Table 7.

TABLE 7

"WHAT ARE YOUR PLANS FOR COPING WITH AN UNANTICIPATED LOSS OF YOUR COMPUTER CAPABILITY?"

Response	Times Mentioned
If it happens, the company is dead	2
We have no plan now and none under development.	10
We have no plan but we are studying the problem.	4
We would ask our vendor for guidance.	3
We have an informal plan involving vendor assistance.	7
We have a formal plan involving vendor assistance.	5
We have a cooperative agreement with another company.	1
We have excess internal capacity available.	3
We operate compatible centers which could absorb the work if any one center goes down.	3
We operate a contingency center for just this purpose.	2

The responses in Table 7 in no way overstate the lack of attention to facility recovery in the companies we visited. From other discussions of the topic during the interview process, we reached a number of relevant conclusions:

- Corporate management generally believes that its computer operations are much better prepared to meet a disaster than is actually the case.

- Although a certain amount of lip service is paid to disaster recovery, most EDP managers are not really uncomfortable with their level of preparedness because they believe that the probability of disaster is extremely low. In addition, given their present budgetary constraints, they consider other problems to be more pressing.

- Either consciously or unconsciously, most EDP managers who rely on "vendor support" for system recovery substantially overestimate the vendor's ability to provide assistance, and they underestimate the time required for and the complexity involved in recovery.

- Almost all attempts to establish intercompany backup agreements have floundered on compatibility and capacity problems.

- Such recovery plans as have been successfully made by and large attempt to reestablish batch operations only, conceding that any recovery of lost telecommunication operations would be a much more difficult problem.

Database Backup and Program Control

Short of a physical disaster that disables the computer, there is still the problem of assuring integrity and continuing operations on a timely basis.

Most of the EDP managers interviewed were reasonably comfortable with their procedures for data recovery. Fewer than 10 percent were not. By far the most common procedure is to "dump" a copy of the protected file on a daily or weekly basis, almost an automatic result in a batch update environment when the next file generation is produced. Such backup files are stored at remote locations varying from "a room across the street" to "a salt mine 100 miles away." All transactions applied to the file between dumps are logged and these are also stored remotely on a regular basis. In the event of loss, a database can be restored by reapplying file transactions to the backup copy. A typical recovery was described as requiring from 20 minutes to one day.

In contrast to their feelings about procedures for database recovery, most managers are uncomfortable about the adequacy of procedures for controlling changes to existing programs. All considered it a significant exposure and most confided that any trusted system programmer could undoubtedly manipulate programs for personal gain.

Even more than embezzlement, however, many managers fear the potential in such an uncontrolled situation for rapid and devastating sabotage by a disgruntled or similarly motivated employee. A question regarding major control over program changes was put directly to the manager. The responses are presented in Table 8. Approximately one third of the managers interviewed stated that program changes could be made only on programs in a test library and that movement of programs into the production library was closely monitored. The existence of this "single door" is thought by some to significantly deter unauthorized modifications.

TABLE 8

"WHAT CONTROLS ARE THERE OVER PROGRAM CHANGES?"

Response	Times Mentioned
Not sure	1
None	2
Little	2
Little control over knowledgeable people	4
Only the analyst or programmer in charge of application can change it	5
User must request any change	4
EDP manager must authorize any change	11
Independent review or dual responsibility for all changes	6
Changes are installed by the operator once each day	3

It is generally believed that unauthorized changes should be detected eventually by the internal audit involvement in the review of program changes, which in the majority of cases was described to us as "none." Specific responses on internal audit's involvement are shown in Table 9.

NEW COMPUTER APPLICATIONS

If the process of developing new computer applications is to include evaluation of all reasonable design alternatives, to document the steps in the selected system, and to assure its usefulness, flexibility and auditability, some formalized procedure to guide the system development effort and to document the results would appear to be in order. When EDP managers were asked what formal development procedures are in fact used, a range of responses was received (Table 10).

TABLE 9

"WHAT IS INTERNAL AUDIT'S INVOLVEMENT IN PROGRAM CHANGES?"

Response	Times Mentioned
None	29
Very seldom	2
Log of changes is available	2
Formally informed	3
They track changes to critical systems	2
They review only major rewrites	2
They review test results	1
They run a sample for review of changes	3
They review at next systems audit	1

TABLE 10

"WHAT FORMAL PROCEDURE IS EMPLOYED IN SYSTEM DEVELOPMENT?"

Response	Times Mentioned
None	9
Not sure	1
Documentation standards in the form of a manual or guide	7
A formal development methodology developed in house	13
An adaptation of a commercially available methodology	6
A commercially available methodology	6

Several managers admitted that control of the development process and preparation of adequate documentation are indeed problems. The demand for experienced EDP professionals is such that they do not take kindly to firm rules, so development and documentation "standards" are often no more than

suggested guidelines. One manager commented: "If I forced them to comply with everything in those manuals, they would quit tomorrow." Some programmers and analysts apparently believe that system development is a creative art form that should not be curtailed by rules, and that system documentation is an unproductive activity reserved for programmer trainees.

Some data processing managers are not completely unsympathetic to that point of view. When asked what they themselves do to sensitize their personnel (analysts, programmers, and operators) and train them in internal control considerations, their responses fell into three categories: (1) nothing, (2) informal and (3) formal training. Frequency responses and selected quotations are presented in Table 11.

TABLE 11

"WHAT IS DONE TO SENSITIZE EDP PERSONNEL TO INTERNAL CONTROL CONSIDERATIONS?"

Response/Quotations	Times Mentioned
We do nothing at all	16
"They know what bad control is."	
"Users consider the audit trail to be nonsense."	
"Controls are not of interest to an EDP staff."	
"What would I train them to do?"	
We rely on informal methods	20
"We rely on on-the-job training."	
"A bad previous experience is the best training."	
"Management emphasizes control all the time."	
"Internal audit reviews and enforces control."	
"User concern with reliability takes care of it."	
There is some type of formal training	8
Outside professional courses, films, audio-visual programs.	

Seminars by internal auditors.

Study of standards manuals.

CONTROL OVER DATA PROCESSING ACTIVITIES OF UNITS AND/OR DIVISIONS

Management control over corporate data processing resources and activities, particularly those outside of the corporate headquarters, varies widely among the corporations interviewed. In 14 corporations, all corporate data processing hardware and staff are under a single corporate officer. In most of these cases, however, the hardware is physically located throughout the corporation. In two of these 14 corporations, some data processing staff are located in divisional units but report directly to corporate management. In all other interviewed companies that use computer systems, the management of data processing is decentralized. Even in the 14 companies where there is centralized management, the centralized management does not include the data processing activities of the subsidiaries.

The degree of decentralization also varies. In 16 companies, the divisional data processing activities are under no direct control of the corporate headquarters. Other organizational structures include the following:

- the hardware is centrally controlled, but the data processing staff reports to division management;
- certain data processing systems are designed, constructed, and operate centrally (e.g., payroll, personnel, and accounting), while others are designed, constructed, and operated by the divisions (e.g., engineering, scientific, and sales);
- all corporate data processing systems and those of selected divisions are managed and operated centrally, while systems of other divisions are managed and operated locally.

Where the management of data processing is decentralized, various policies and procedures exist to provide some form of centralized control over decentralized activities. Included in these are the following:

1) review and/or approval of proposals for new hardware;

2) review and/or approval of proposals for new EDP systems;

3) yearly or ongoing review of all activities;

4) corporate standards for hardware and EDP systems;

5) common operating systems and/or database management systems;

6) common EDP systems which are used at the option of the division.

In almost all cases, the corporate data processing manager expressed much more confidence in the internal control aspects of the headquarters activities than of the divisional activities. In several cases, the manager was completely unable to assess the control characteristics of the divisional activities.

USE OF EXTERNAL RESOURCES FOR EDP SUPPORT

Many corporations rely on outside sources for data processing resources and/or services. These external sources may supply people (programmers, analysts, operators, etc.), special programs and data, and/or computer facilities. Only four data processing managers were aware of sensitive data or programs being maintained by or accessible to external sources. The sensitive information is in the areas of product formulas, personnel data, financial data, and engineering design programs and data. However, in many cases where outside sources are being used, the data processing manager admitted that he was not necessarily aware of all of the uses of external sources.

The data processing managers were asked to describe the measures taken to insure the confidentiality of the programs and data placed on external machines. The responses included the following:

- encoded data;
- reputation and word of vendor;
- responsibility of the department that uses the external source;
- confidentiality agreement signed by the vendor;
- vendor's financial liability for confidentiality.

Several data processing managers related that they are in the process of moving all data and processing in-house. They listed security and reliability among the reasons for this action. Six of the managers stated that there were no controls, no testing or audit of controls, or that they had no knowledge of the existence of controls in external systems. Several managers also indicated a belief that external sources are often used to avoid the control mechanisms of the company. When an external facility or service is used, formal standards and procedures can be avoided, and the controls normally required in in-house systems can be omitted. This avoidance of controls through the use of external sources was often attributed to divisional data processing activities.

SELF EVALUATION

During the interview, EDP managers were asked to rate the internal control aspects of data processing in their own company with that of other companies in their industry. By and large, the managers rated themselves generously, as seen in Table 12.

TABLE 12

"HOW DO THE INTERNAL CONTROLS IN YOUR EDP OPERATION COMPARE WITH THOSE OF OTHER COMPANIES IN YOUR INDUSTRY?"

Rating	Times Mentioned
The best in the industry	2
By far the best in the industry	12
Above average	12
Average	10
Below average	4

On the basis of our own interviews, we would have rated some of those who considered their operations only average as much better; we thought that some others overrated themselves considerably. One manager, who accurately placed his organization

in the below average group, made the interesting observation that while his operation was possibly "lacking in control," it is "easy to use."

INTERNAL CONTROL EXPOSURE

Data processing managers were asked to identify what they considered their own major concerns about internal control. What sort of problems worry them the most? The responses divide roughly into five categories: loss of computer usage; control of rapidly developing technology; security; control standards and procedures; and operational concerns. Table 13 presents frequencies and specific items under each heading.

TABLE 13

"WHAT ARE YOUR MOST SIGNIFICANT INTERNAL CONTROL CONCERNS WITH RESPECT TO DATA PROCESSING?"

Category/Specific Items	Times Mentioned	
Loss of computer usage		13
Facility backup and recovery	9	
Power supply disruption	1	
File recovery	3	
Control of rapidly developing technology		8
Proliferation of minicomputers and distributed systems	1	
Access control in online interactive systems	2	
Corporate dependency on communication lines	2	
Impossibility of controlling large, new, complex, volatile systems	3	
Security		7
Physical security	3	
Data access	3	
System access	1	
Control standards and procedures		19
Lack of formal documentation and standards	3	
Lack of definition of meaning of control	2	
Inability to certify existing programs	8	
Lack of accounting training in EDP personnel	1	
Lack of separation of duties in EDP	2	
A single trusted employee can do great harm	3	

Operational concerns	7
Accuracy of data	2
Long system development lead time	1
Dependency on key people	1
Quality of staff	1
Efficiency of current system	1
Lack of long range plan	1

ROLE OF INTERNAL AUDIT IN EDP CONTROL

The internal audit function in many companies plays a significant role in the development and review of both the internal control environment and the internal control procedures utilized by a company. As EDP systems become a more important and visible component of internal control systems, the role of internal audit in the implementation and operation of EDP systems should receive increased attention. The interview guide was therefore directed toward (1) the various kinds of internal audit involvement in the development of EDP systems, (2) the EDP manager's assessment of internal audit's knowledge of data processing and the effectiveness of internal audit's involvement in EDP system development, and (3) the possibility of obtaining increased participation by internal audit in EDP development.

The involvement of the internal audit staff in EDP systems varies widely from organization to organization. Our review of this involvement has identified the following four functions or roles for the internal auditor:

- participation in the specification, design, and implementation of an EDP system;
- participation in the audit of an operational EDP system in the normal course of an audit of a functional area of the corporation;
- participation in the specification of standards for EDP systems and in the specification of standards for the control of EDP.
- review of the physical facilities.

Internal Audit Involvement in Development of EDP Systems

Electronic data processing systems experience a "life cycle" that includes some or all of the following steps:

- user's assessment of need;
- feasibility study of meeting user's need at acceptable cost;
- determination of system specifications, including provision for controls;
- development of programs and files to meet specifications;
- testing and approval of programs, files, manual procedures, etc.;
- implementation;
- continuing review, maintenance, and modification;
- major revision or abandonment.

From a control point of view, the crucial steps in this life cycle are the third (determination of system specification and provisions for controls), the fifth (testing and approval of the program, files, manual procedures, etc.), and the seventh (continuing review, maintenance and modification). Data processing managers were asked the extent of internal audit participation, especially in these crucial phases of system development.

Internal auditors are sometimes not involved at all in EDP system development projects. If they are involved, it tends to be (1) in large projects, size often being determined by dollar cost (e.g., over $50,000 or over $100,000), (2) in projects having financial aspects or ramifications, (3) in asset management systems, and (4) sometimes in systems selected to stimulate control consciousness

regarding all system development activities.

Of the EDP managers interviewed, 33 indicated there is some involvement of internal audit in the development of specific systems. The degree of involvement varied considerably and rarely included participation in all three of the important phases mentioned above. Less than one fourth of those queried stated that internal audit was involved in an official sign-off procedure before the system becomes operational.

Thirty-eight EDP managers asserted there is no involvement of internal audit in the maintenance and modification of systems after they are placed in operation. In some companies, internal audit tracks the changes in "critical" systems or audits the specific changes that are reported to it.

Post-Implementation Audits by Internal Audit

EDP systems which are a part of the control system of a functional activity of the company tend to receive more attention. In response to a question about the post-implementation review of EDP systems, most managers indicated that "critical systems are audited by the internal auditor." (Detail is presented in Table 14.)

TABLE 14

"TO WHAT EXTENT ARE EDP SYSTEMS AUDITED?"

Response	Times Mentioned
Critical systems are audited by the internal auditor	30
Critical systems are not audited by the internal auditor but are audited by the external auditor	3
Critical systems are not audited by the internal auditor but are audited by government auditors	3
Critical systems are not audited by the internal auditor but are audited by EDP auditors in the data processing department	1
Critical systems are not audited	5

In companies where internal audit does review the system after it becomes operative, the procedure for selecting systems to be audited varies. In 16 companies, the EDP manager was not aware of how systems are selected for audit. In the remaining companies, the bases most commonly utilized in selecting systems for audit were the amount of resources controlled, the financial risk, the number of complaints received, the ability to improve operational effectiveness, requests by the user of EDP, and a regular rotation procedure.

A number of methods of audit are available. The EDP manager's assessment of the procedure followed by internal audit focused on the software portion of the system (Table 15).

TABLE 15

"WHAT IS THE FOCUS OF INTERNAL AUDIT'S EDP REVIEW?"

Response	Times Mentioned
Formal procedures	3
Special software developed by internal audit staff	12
Programs written by EDP staff to assist in the audit	2
Traces flowcharts only	1
Inspects the audit trail of selected EDP systems	1

In addition to their involvement in the development and post-implementation review of EDP systems, the internal auditors in some organizations perform other functions related to EDP systems. These functions include:

- reviewing systems standards developed by the EDP department;
- serving on a standing review committee of the data processing department;
- auditing the activities and operations of the data processing department;
- assisting corporate data processing in informing the divisions of the need for control in EDP systems;

- reviewing the physical security of the hardware system;
- reviewing the recoverability of the hardware system;
- serving on review committees for specific EDP systems; and
- reviewing the security of a specific EDP system.

EDP Managers' Assessment of the Quality of Internal Audit Involvement

In addition to determining the degree of the internal auditor's involvement with EDP, the interview was used to assess the EDP managers' assessment of the quality of this involvement. On the basis of responses to a direct question about the internal audit staff's knowledge of EDP, the consensus was that it is inadequate (Table 16).

TABLE 16

"WHAT IS YOUR ASSESSMENT OF INTERNAL AUDIT'S KNOWLEDGE OF EDP?"

Response	Times Mentioned
Sufficient	3
Not enough	11
Very little	8
None	11
Do not know	2

The effectiveness and quality of internal audit participation, as seen by the EDP manager, varied all the way from "professional, competent, and reasonable" to "they cannot detect the lack of controls in an EDP system nor the circumvention of those controls." Of the companies where internal audit is involved with EDP systems, only about one third of the data processing managers had a positive opinion about the effectiveness and quality of the involvement. These positive opinions were often based on good communication between the two groups and common belief in the need for secure, cost-beneficial EDP systems. In other cases, the positive opinions were based on the successful performance

by internal audit of some specific functions with respect to EDP systems.

Negative opinions about the quality of the internal auditor's activity on EDP systems included criticism of the internal auditor's knowledge of EDP and of the business of the corporation, as well as criticism of the timeliness and intensity of the internal auditor's EDP involvement. Specific criticisms questioned the internal auditor's ability to determine what controls should go into a system, to detect controls within a system, and to detect if these controls had been or could be circumvented.

Special circumstances often influenced the views of the EDP managers interviewed. In some companies, no new systems had been developed in several years. In others, EDP had its own internal audit staff which had little relationship with the company's internal auditors. In still other companies, personnel changes, publicity surrounding a computer fraud, or special interest by the Board of Directors influenced the extent and quality of internal audit participation in the development of EDP systems.

Problems Involved in Increasing Internal Audit Participation

When asked to describe reasons which might prevent effective future internal audit involvement in the future development of EDP systems, data processing managers were less optimistic. Their responses covered a considerable range and included the following thoughts:

- "The demand for auditors with a good understanding of EDP far exceeds the supply."
- "Our internal audit department does not attract energetic and creative people."
- "Because the turnover in internal audit is so low, there is little chance to replace auditors with no knowledge of EDP with auditors who do understand it."
- "Internal auditors who do have a thorough knowledge of EDP often leave and transfer either to data processing or to some user department. There is too little room for advancement within internal audit."

- "It is unreasonable to expect someone to be knowledgeable in the standards and practices of both auditing and EDP."
- "The very concept of an EDP auditor is bad; all auditors should become familiar with EDP technology and EDP systems."
- "It is hard to justify tying up a qualified systems analyst from data processing just to review a system design with someone from internal audit."

External Auditor's Role in EDP Internal Control

Does the work of the external auditor in the annual financial audit compensate for possible deficiencies in the EDP competence of or coverage by company's internal auditors? Conversations with EDP managers indicate that this is certainly not the case for most companies. External auditors are required to test only those system controls upon which they plan to rely when rendering an opinion of the "fairness" of the company's financial statements. They tend either to validate a limited number of systems thoroughly each year, or to review a larger number of systems less thoroughly. In some cases, they review only system documentation and do not audit the actual programs at all. Some use special proprietary programs and questionnaires to test EDP systems.

External auditors may also direct attention to important matters that have received less attention than they deserve, such as the physical security of the system, or the need for procedure manuals in the data processing department.

When asked to evaluate the knowledgeability of the external auditors and to rate their work, EDP managers were not much more complementary than they were when discussing the work of internal auditors. In some cases, the external audit staff was rated highly. But in the majority of cases, both their knowledge of EDP technology and the thoroughness with which they undertook their examinations were seriously questioned.

4. Basic Conclusions and Recommendations

The data and observations collected during our interviews combine to yield an inescapable conclusion. The continuing technological development of electronic data processing, the shortage of qualified EDP professionals, the substantial costs involved, the utilization of EDP to control function activities, and the difficulty management faces in understanding and evaluating the attendant risks make internal control over EDP activities a problem for all corporate executives and especially for those responsible for EDP administration.

Our analysis of EDP control concerns shows the problem to have four facets:

1. The protection of EDP resources to avoid sabotage, unwarranted access, theft, misuse, or abuse of any kind.
2. The maintenance of EDP systems in use to assure that changing needs are met and controls are maintained.
3. The initiation of new EDP systems to assure that full advantage is taken of new technology and the computer's control capacity.
4. The development of new EDP systems via processes which assure that users' needs are met economically and that desirable controls are built into the system.

In general, five groups share responsibility for control of EDP activities: functional users of EDP services, the EDP staff itself, internal auditors who monitor controls throughout the company, general management which, under the Foreign Corrupt Practices Act, has ultimate responsibility for internal control, and independent accountants who review internal control in connection with their annual audit of the company's financial statements.

No one of these groups is in a position to have complete control over all aspects of EDP control. Our interviews revealed a wide variety of political interests and confusion with respect to allocation of responsibility. The five groups were often ill-informed of each other's EDP-related activity, and generally no one group was aware of the full range of EDP control issues warranting attention.

Consequently, the probability of satisfactory control over electronic data processing is low indeed. The problem is further compounded by the speed of technological development, the specialized language of data processing, and the general aura of mystery that surrounds EDP.

By its nature, EDP is difficult to control, so it is not surprising that we found very few companies in which EDP functions could meet a strict interpretation of the accounting provisions of the Foreign Corrupt Practices Act. Yet there are some steps that can and should be taken to improve control over EDP activities in almost any company. Leadership within a company is much needed for this purpose. But no single interest in data processing appears to have all the necessary managerial authority, EDP know-how, and appreciation for internal control. Unless such a combination is found in one person, leadership may be possible only from a carefully constituted committee. That committee should undertake some of all of the following activities:

1. Analyze the total range of EDP activities for control points that warrant attention, and then seek corporate policy that fixes responsibility for each of these.
2. Analyze present operational systems, determine what reviews by users or internal and independent auditors would be useful, plan a review schedule, and urge that management adopt it.
3. Review the physical control over EDP hardware and software and the accessibility of information in the EDP files to unauthorized personnel and to those not needing access, and take necessary measures to provide adequate protection.
4. Review EDP back-up and recovery plans, develop minimum financial needs, and seek adequate funds.
5. Determine needs of EDP staff for training in control practices and purposes, and seek commitment to a training program.

6. Determine the needs of internal auditors with respect to training in EDP concepts, functions, and goald, and seek commitment to appropriate hiring and training programs.

7. Consider the most probable variety of EDP systems to be required within the foreseeable future; consider similarities and dissimilarities and desirable control features; and propose reasonable standards for the initiation, development or acquisition, installation, operation, maintenance, and termination of these systems within all operating divisions of the company.

While managerial authority for several of these actions clearly resides with top management, we believe that the initiative for action must come from the data processing executive. Data processing is at the root of the problem. It is data processing that possesses and applies that mysterious language and technology that baffles others in the organization. EDP specialists have traveled too far too fast for the others to keep pace. As a part of management, they have a responsibility to see that their expertise contributes to the total health of the company, not just to one aspect.

In brief, we urge data processing managers to take the initiative to accomplish the internal control improvements described above. While the development of sound control policies must be a joint management effort, the initative belongs to data processing. Only when such policies are established can data processing be assured that continued technological progress will not be constrained by those who see it as a threat to control.