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

August 1981

DATA PROCESSING CONTROL:
ARE COMPUTER PROFESSIONALS DOING THEIR PART?

Working Paper No. 273

Alan G. Merten

Carol E. Shulman

The University of Michigan

FOR DISCUSSION PURPOSES ONLY

Data Processing Control:

Are Computer Professionals Doing Their Part?

Alan G. Merten

Carol E. Shulman

The University of Michigan

Abstract

While the expanded use of computer and information technology has often brought major benefits to organizations, it has also resulted in significant dependency on these technologies and at least the potential for new and significant internal control risks. This paper presents a framework to analyze these risks, the procedures that an organization can adopt to minimize the risks, and the key people in the organization that influence the quality of the control environment and system. An action plan to assess and improve data processing control is presented.

Key words and phrases: data processing, control, internal control, auditing, system life cycle, risks

CR Categories: 2.4, 3.5

Authors' address: Graduate School of Business Administration,
The University of Michigan,
Ann Arbor, Michigan 48109

Introduction

Internal control over computer resources is a growing management concern. The reasons for this concern are straightforward: (1) Investment in these resources is large and growing. (2) Computer systems increasingly are used as internal control mechanisms over other activities, from production lines to purchasing, through budgeting and strategic planning and more. (3) Current data processing control practices are alarmingly poor. Even well-known techniques such as separation of duties, proper documentation, system access passwords, batch totals, and audit trails remain surprisingly underutilized. (4) The Foreign Corrupt Practices Act (FCPA) of 1977 makes corporate executives legally responsible for maintaining "reasonable internal accounting control." As many corporations rely heavily on computer systems for accounting and other financial activities, the FCPA could be construed to make executives liable for breakdowns in data processing control.

The trends do not bode well for improving control. Organizations will continue to face business problems and opportunities which can be addressed by more effective use of information technology. Computer systems can continue to result in better decisions, increased productivity, and improved market and financial performance. But the flip side of the coin is increasing exposure: the organization becomes even more dependent on computer systems, and thus both the opportunity for and the potential impact of computer fraud or failure grow also. To compound the problem, information technology changes swiftly--usually far more rapidly than our recognition of the accompanying risks, and the design and use of suitable controls. It's no wonder executive management is greatly concerned.

The remainder of this article describes the breadth and depth of the world of data processing control. It discusses why data processing professionals should be concerned about their organization's exposure to loss through its use of computer systems. It concludes with why and how data processing professionals can and should lead the effort for improved control in their company.

DATA PROCESSING CONTROL IS A BROAD SUBJECT

Risk management is an integral part of doing business. Risks are usually classified into two groups: those arising from factors mostly beyond the organization's direct control, such as the political and macro-economic climate (external risks), and those attributable to factors well within the organization's domain, e.g., its personnel, financial policies, and so on (internal risks).

"Internal control" may be defined as the body of formal or informal plans, policies, and procedures which a firm employs to minimize internal risks. Note the use of "minimize" rather than "eliminate" in this definition. Proper control is financially rational. That is, it balances risk reduction against the cost to achieve it.

Most organizations have complete authority over their acquisition and use of computer systems. Risks which arise from computer use are therefore internal risks, so data processing control is properly classified as a subset of internal control. The authors suggest the following broad definition of data processing control:

> Data processing control comprises the body of formal or informal plans, policies, and procedures employed by an organization to ensure that appropriate data processing resources are available, and that the organization derives the maximum legitimate, cost-effective benefit from their use.

A complete enumeration of data processing risks and control techniques is beyond the scope of this article. Figures 1-4 provide an overview of various aspects of the area. Figure 1 gives some examples of losses that data processing control practices should seek to minimize. Figure 2 classifies the sources of risk, and gives some examples of exposure from each source (notice how these risks permeate every phase of the system life cycle). Figure 3 enumerates the many potential participants in data processing control. Figure 4 provides a taxonomy for the many control techniques in use.

Figure 1. Some Examples of Data Processing Loss

1. A development project goes way over budget.
2. Maintenance programming consumes too much staff time.
3. Someone sells confidential data to a competitor.
4. A disgruntled employee destroys programs or data.
5. A fire in the computer room destroys equipment.
6. A power outage causes downtime.
7. Hardware/software is acquired that proves inadequate to its task.
8. Fraudulent transactions or programming cause loss of other assets.
9. Employees play computer games on company time and equipment.
10. The company's sales volume is constrained by the capacity of the order processing system.
11. By the time a new system is installed, it isn't needed anymore.
12. A system crash or operator error destroys a data base.

Inadvertent Error
- Planning/Problem Analysis
- Design
- Programming
- Data Entry
- Operator
- Documentation

Hardware Failure
- CPU failure
- Data storage error
- Power fluctuations
- Power failure
- Peripheral failure
- Communications failure

Deliberate Misuse
- Fraudulent transactions
- Fraudulent programming
- Theft of data, programs, or hardware
- Unauthorized use of DP resources

Natural Disaster
- Fire
- Flood
- Storm

Sabotage or Armed Conflict
- Deliberate destruction of hardware/facilities
- Deliberate destruction of software/programs
- Accidental destruction during civil insurrection or other armed conflict

Figure 2. Causes of DP Loss

Figure 3. Potential Participants in Data Processing Control

1. Chief Executive Officer

   Promotion of control consciousness and setting of high-level goals and policies to guide computer use.

2. Chief Financial Officer

   Almost always responsible for control of financial systems and for the internal audit function. Often involved in computer procurement.

3. Data Processing Officer

   Data processing personnel policies, plans, and priorities; distribution of duties; promotion of control consciousness; imposition of standards and procedures; monitoring of control performance; procurement.

4. Data Administrator

   Definition, modification, and access to machine-readable data; protection of machine-readable information assets.

5. Other Data Processing Staff

   Compliance with standards, promotion and display of control consciousness, assistance in monitoring control, development of control mechanisms, working effectively and efficiently.

6. Internal Auditor

   Monitoring of data processing control; often involved in systems design, testing, planning to ensure that adequate controls are present.

7. External Auditor

   Some monitoring of data processing control, in general, but mostly as it relates to systems material to the production of external financial reports.

8. Users

   Data processing planning and priorities, control requirements in specifications, procurement, monitoring and assessing control, assisting in design, testing. Sometimes end user is also operator, and therefore may be responsible for meeting certain Input-Process-Output controls.

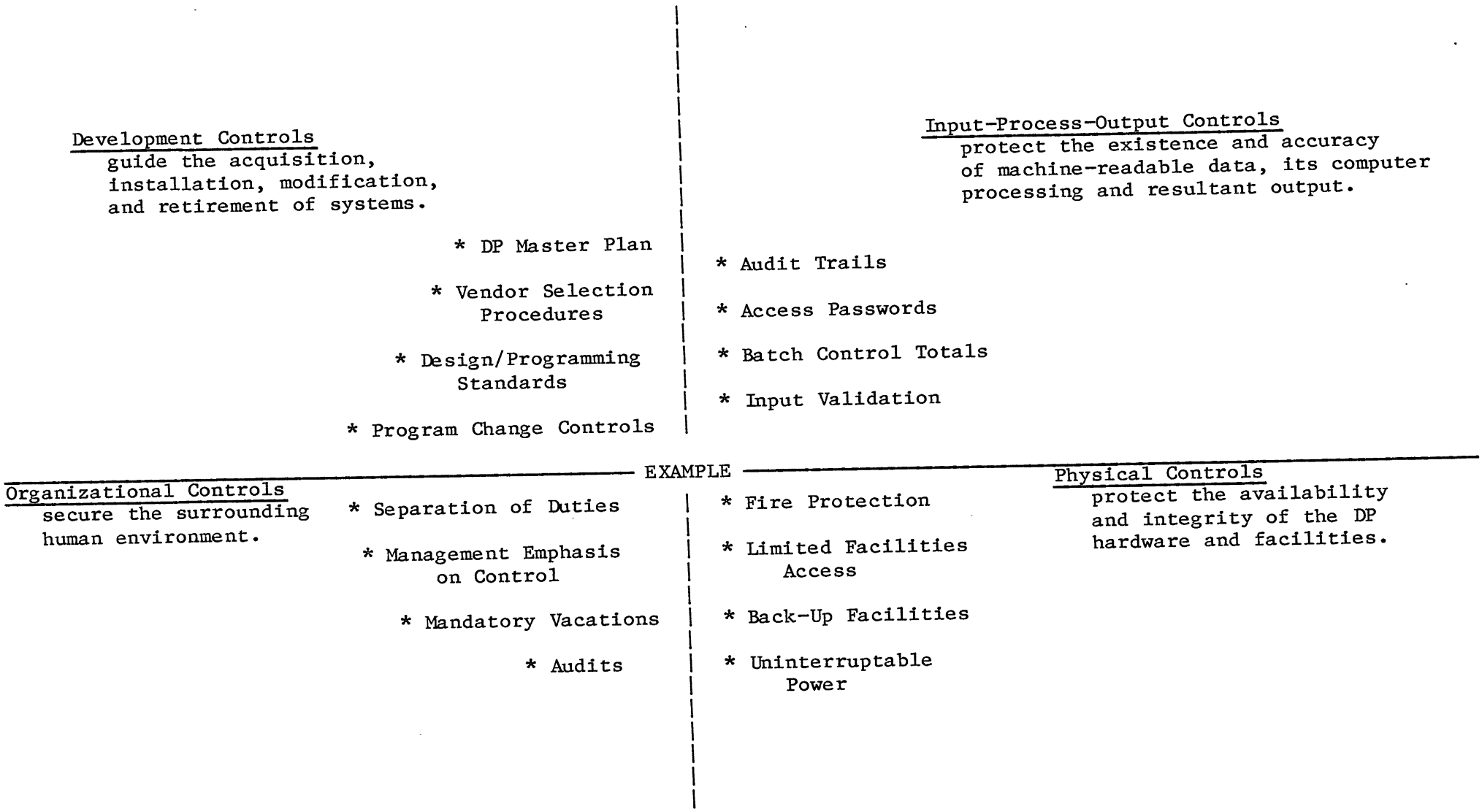

Figure 4. Control Taxonomy

WHY DATA PROCESSING PROFESSIONALS SHOULD GET INVOLVED

There are several compelling reasons why DP professionals must participate in, if not lead, the effort to improve data processing control. Some of these appeal to our own self-interest, others to higher ideals: (1) Someone is going to do something soon, even if we don't; (2) that something--regardless of who does it--will probably affect our jobs and career paths; (3) our expertise is desperately needed; and (4) our professional image would be enhanced by our leadership.

We have already established that general management at the highest levels is legitimately and increasingly concerned about the current state of data processing control. This concern can only spread, especially as more and more people experience or learn about incidents of control breakdowns. Stockholders, government, and the general public may be expected to exert more and more pressure on management and on our profession to improve our control performance. If we fail to do so of our own accord, we can expect them to try to do it for us.

It is also clear that in order to improve control, changes must be made in the way we work. Among the obvious changes will be: (1) An explicit assignment of control responsibilities to data processing managers, analysts, programmers, and operators. (2) A corresponding change in the way we are measured, with increasing emphasis on control and decreasing emphasis on fast delivery, low-cost operation, and ease of use. (3) We will become more integrated with other company activities, because good control is organizationally dependent--if we don't know our firms, we can't know what constitutes good control. In addition, the job is too big for us to handle alone, especially at first; we will need help from other parts of our organizations.

These are only a few examples of changes that will or could be made to our environment. It is in our own interest to be involved in specifying them.

On a less selfish note, we obviously have a lot to contribute. Computers are still a mystery to many outside our profession. Senior management needs and wants help achieving better control. Our knowledge of current and future computer and information technology, our skills in problem analysis, systems design, programming, and operations--these are tools which are necessary, and which we are best able to supply. Poor data processing control obviously has the potential to cause society much grief. We can, more than anyone else, contribute to the elimination of the threat.

Lastly, we are rightly or wrongly often considered part of the problem. Here are a few examples of ways in which we are perceived to, or actually do, hamper data processing control: (1) Many of us believe system development is an art that should not be subject to rules, standards, or procedures. (2) We rarely document our work adequately, and often view documentation as unproductive and/or beneath us. (3) We are often perceived as having more loyalty to technology than to our employers (our rapid turnover doesn't help). (4) We have let such an aura of mystery persist about computers that few outside our industry truly understand what we really do. We are perceived as being in a position to do great harm should we be so motivated.

Active leadership from the DP profession in the fight for better data processing control can go far to erase many of these negative stereotypes. With it, we demonstrate we do have higher loyalties than to our technology alone, that we do care about our contribution to our organizations and to society. We demonstrate that we can and will control our own activities without coercion. And, in taking leadership, we broaden our own career paths

and maintain control over our own professional destinies. In short, we have much to lose by inaction, and more to gain by leadership.

WHAT YOU SHOULD DO

We believe that the following should be your initial goals in starting down the admittedly arduous road to improved control over data processing:

(1) To educate the data processing and internal audit staffs, users, and senior management about data processing risks and controls, and the monitoring of same.

(2) To identify who is currently responsible for the various facets of data processing control, to evaluate the effectiveness and appropriateness of such a distribution of control responsibilities, and to make immediate changes in assignments as necessary.

(3) To establish an explicit, well-publicized management policy on control over the acquisition, allocation, and use of data processing resources. This policy will guide the development of relevant, cost-effective control standards.

(4) To catalog the various data processing resources (hardware, software, communications, development methods, applications, and personnel) on which the organization's current and foreseeable future success materially depends; to enumerate the risks inherent in such dependence and the current control over these risks, and to assess the adequacy of existing controls.

Ambitious as these goals may seem, we believe that most organizations could meet them within three to four months by following this action plan:

(1) Form a committee/study group of 10 to 15 people representing data processing operations, development, user groups, internal audit, and senior management.

(2) Embark on an 8 to 10 week education program.

(3) Perform a 100 to 200 hour initial assessment of data processing exposures and current control practices.

The Committee

A major barrier to rational data processing control in most organizations is that there is no locus of the required knowledge and skills. Data processing professionals understand the technology but have little background in risk management, internal auditing, financial analysis, or strategic planning. The Internal Audit department possesses many of these skills, but knows little about computer systems. And so on. Yet, these skills and more are required. In the long run, organizations should strive to cultivate personnel with more of the requisite skills. In the short run, however, an interdisciplinary approach is required.

A committee can be used to bring together a group of individuals, none of whom alone possesses all the required expertise, but who together supply the needed talents. Such a group would ideally consist of data processing employees such as senior systems analysts or others with a broad knowledge of the organization's use of computer systems. It should contain representatives of computer facility management. Naturally, such a team must also include members of the internal audit staff since data processing monitoring closely parallels other types of management auditing. Managers of areas which make substantial use of computer systems in their planning, analysis, or operations should also be members, or at least available as needed. At least one representative of senior management must also be a member; we suggest that the vice president of finance has the most to contribute.

The Education Program

The first task of the committee is to educate itself. This can be accomplished relatively easily in 8 to 10 weeks by leveraging the expertise the committee contains. Figure 5 suggests a bibliography for various members. Internal auditors read the data processing control literature which requires a knowledge of auditing techniques, and deliver a one to two hour tutorial, summary presentation on this material to the rest of the committee. Data processing professionals read the literature which requires data processing expertise, and prepare a similar report; and so on.

This program should require a regular commitment of 6 to 8 hours per week per member for 8 to 10 weeks, with an additional 7 to 12 hour commitment required during one week from members who will make presentations. While this amount of time is substantial, it is not inordinate, and it is an absolutely necessary investment.

The Study

The education program outlined above provides the necessary foundation to perform an effective assessment of data processing control in 100 to 200 work hours. This assessment culminates in a written report which recommends the next series of steps that should be taken.

We suggest the study begin by reading company documents and conducting interviews as necessary to gain the following information:

Burch, J. G., and Sardinas, J. L. "Computer Control and Audit: A Total Systems Approach." New York: John Wiley and Sons, 1978.

Canadian Institute of Chartered Accountants. Computer Control Guidelines and Computer Audit Guidelines. Toronto: 1970.

IBM. Management Controls for Data Processing, GF20-0006-1, 1976.

IBM. Staying in Charge, G505-0058-0, 1980.

Krauss, L. I., and MacGahan, A. Computer Fraud and Countermeasures. Englewood Cliffs, N.J.: Prentice Hall, 1979.

Litecky, C., and Rittenberg, L. "The External Auditor's Review of Computer Controls." Communications of the ACM, May 1981, pp. 288-295.

Mautz, R., et al. Internal Control in U. S. Corporations: The State of the Art: Financial Executives Research Foundation, New York, 1980.

Merten, A., and Severance, D. Data Processing Control: A State-of-the-Art Survey of Attitudes and Concerns of DP Executives." MIS Quarterly, June 1981, pp. 11-32.

Rittenberg, L. E., and Purdy, C. "The Internal Auditor's Role in MIS Developments." MIS Quarterly, December 1978, pp. 47-58.

Stanford Research Institute. Systems Auditability and Control Study (Executive Report, Data Processing Control Practices Report, and Data Processing Audit Practices Report) Altamonte Springs, Fl.: Institute of Institute of Internal Auditors, Inc., 1977.

Touche Ross and Company. Computer Controls and Audit. New York: 1973.

Figure 5. Data Processing Control Literature

(1) Control Responsibilities: Who has formal, informal, or perceived control over data processing resources and data processing systems? With respect to the phases of the system life cycle, who has the responsibility in each phase to: (a) identify risks, (b) develop suitable controls, (c) operate controls, and (d) monitor control compliance?

(2) Use of Computer and Telecommunication Technology: Upon what hardware, software, communications, applications, facilities, methods, and data processing personnel do various company operations depend?

(3) Control Techniques: What policies and procedures are in existence to control the building, testing, and evolution of computer systems and to insure that the proper controls exist in computer systems?

(4) The Organizational Climate: What is the level of awareness of data processing risks in users, data processing and audit staffs, and senior management? What are the company's short-, medium-, and long-range business goals? What is the company philosophy? management style? Control policies and procedures will be effective only to the extent that they are consistent with the organizational climate.

A useful way to organize this fact finding is to develop a list of questions, then a list of documents and individuals who might possess answers. The questions can then be organized into interview guides for each interviewee, and into study guides for the document reviews. We recommend that at least two committee members review each document, and that two people perform each interview. Transcripts from recorded interviews may be particularly useful in the assessment, especially if questions are open ended.

Figure 6 shows a suggested organization for the final report. Note that it begins with an executive summary. This section should summarize in two to three pages: (a) the goals, scope, and methods of the investigation; (b) general control strengths and weaknesses; and (c) recommendations for immediate

and near-term actions to improve deficiencies. It is crucial that this summary be distributed among senior management. Other possible recipients include data processing, internal audit, or user personnel who are not on the committee, but who should be informed. The goals of the report are:

(1) to raise the awareness in readers of data processing risks faced by the organization;

(2) to offer specific recommendations for actions to improve control where it is weak;

(3) to motivate the allocation of sufficient resources for the continuing development, operation, and monitoring of properly controlled systems.

Figure 6. Suggested Final Report Format

1. Executive Summary. Two to three pages summarizing the study goals, methods, and recommendations.

2. Introduction. Expanded discussion of study goals, scope, and methods, with a summary of problems uncovered, alternatives analyzed, and recommended actions.

3. Organizational Climate. Enumeration of short-, medium-, and long-range business goals, identification of unique characteristics of the firm within its industry. Description of management style (e.g., formal/informal, centralized/decentralized, etc.). Description of the level and extent of data processing control consciousness.

4. DP Use. An enumeration of the various data processing resources available to the firm, and the uses to which they are put in various operating units within the company. This should take into account any plans for changes in resources or their application. Resources must include those supplied by external sources such as timesharing vendors, software development houses, and so on.

5. Control Responsibilities. Description of the organizational structure as it pertains to control and monitoring of control over data processing facilities, activities, and systems, and in all parts of the firm.

6. DP Risks. Description of the risk identification and evaluation process in use. Enumeration of risks--both controlled and uncontrolled--inherent in the firm's use of data processing.

7. DP Controls. An enumeration of the formal and informal plans, policies, and procedures used to control the acquisition and use of data processing resources.

8. Analysis. Identification of major strengths and weaknesses in the control environment. Identification and evaluation of alternatives for alleviating weaknesses.

9. Recommendations. Description of suggested actions classified as immediate, near-term, and long-term.

10. Appendices. Compilation of interview guides and transcripts, study guides, bibliographies, and other background or detailed information.

SOME CONTROL RECOMMENDATIONS

We feel confident that many who perform the assessment outlined above will find they suffer some of these control problems:

(1) Low level of "data processing control consciousness."

(2) No clear locus of responsibility for data processing control.

(3) No comprehensive life-cycle methodology, policies, standards, or procedures.

(4) Inadequate resources to develop, install, operate, and monitor properly controlled systems.

What constitutes rational control in one organization may prove completely inappropriate in another. This organizational dependence not withstanding, the following suggestions may prove useful as a basis for curing the common control problems just listed:

(1) Raising Control Consciousness: In order to achieve control, it is necessary that all participants be aware of the need for it. Users, data processing staff, and company management must all be aware that risks exist, that controls can and should be implemented to cover them, and that this will necessitate changes in the way systems are procured and used. Several means exist to this end. Among them are the creation and distribution of an explicit policy on data processing control from senior management, circulation of the initial assessment and other reports by the control committee, and a

series of seminars drawn from the committee education presentations. Seminar attendants could include users, vendors, management, DP staff, internal and external auditors.

(2) Assignment of Control Responsibilities: You will probably find that many managers are unable to name the person or persons responsible for a breakdown in data processing control. Among those who have answers, you will find substantial disagreement. Yet explicit assignment of responsibility and concomitant authority is crucial, especially when so many possibly competing interests are involved. We offer the following suggestions for assigning control responsibility:

(a) An information systems audit function should be staffed and funded if none now exists. It should contain a minimum of two people, one a competent internal auditor and one a senior systems analyst or other data processing professional, both with substantial company experience. It should be responsible for verifying that rational controls are embodied in new systems, facilities, and applications; monitoring compliance with controls; and auditing material systems and facilities periodically for efficient and accurate operation.

(b) Since the design and day-to-day use of controls must be independent of their audit, an organization may find it necessary to create a Data Processing Control function reporting to the senior data processing executive. Figure 7 depicts one potential structure for a mature data processing control department in a larger corporation. The Documentation Control group is staffed by technical writers and management, and is responsible for the production, distribution, and maintenance of user, system, and program documentation. The Log Control group is responsible for verifying and archiving operating logs (e.g., error, control total, hardware downtime logs). The Development group

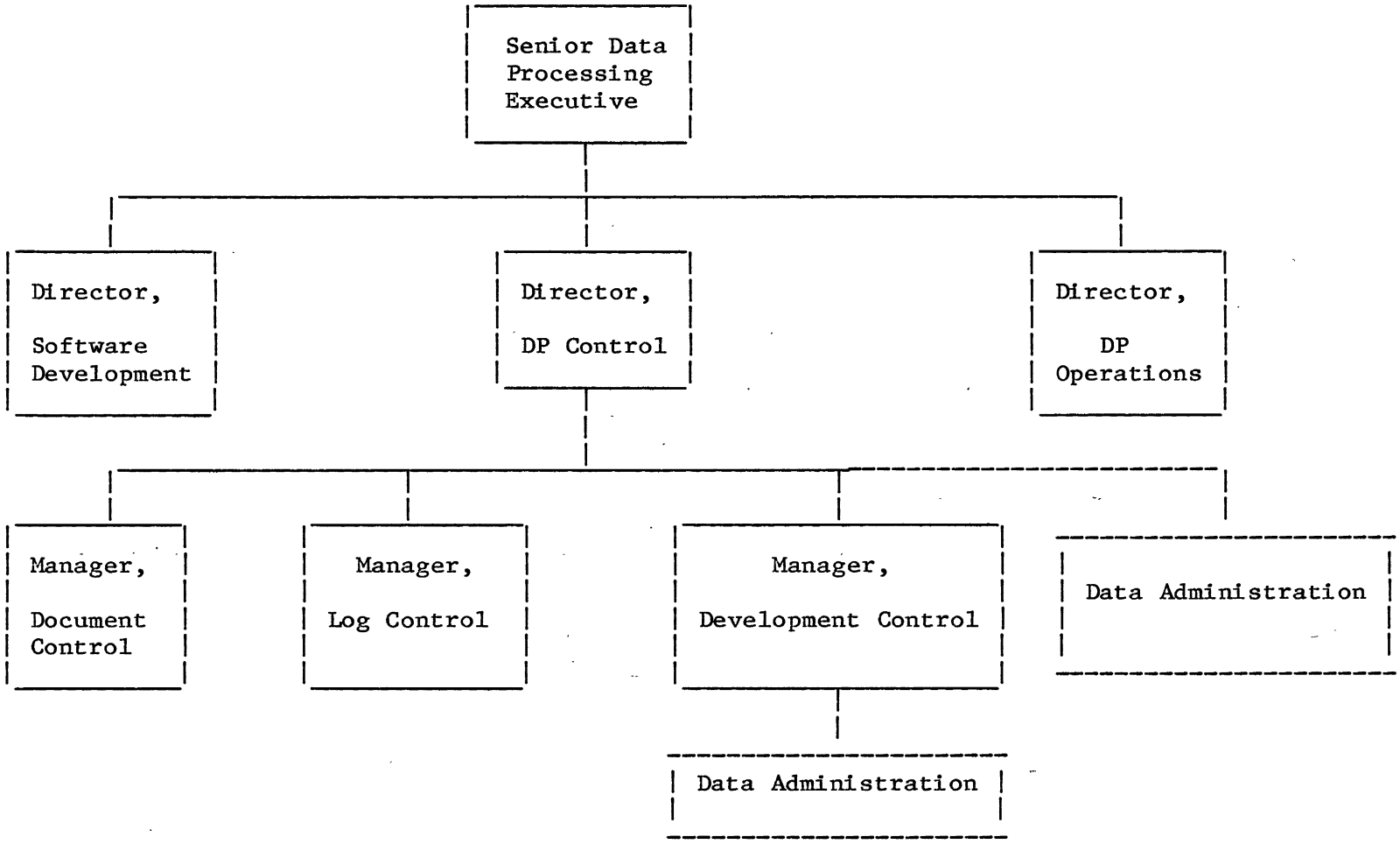

Figure 7. Mature EDP Control Function for Larger Organization, with Two Possible Placements for the Data Administration function.

is responsible for insuring that new systems specifications and designs include a rational level of controls. One can argue that the Data Administration function properly belongs in this domain.

These positions are shown reporting to a Control Director who is peer to the Direction of Operations, Director of Systems Development, etc. One of the Director's key duties is to coordinate control activities with other data processing functions.

(c) Smaller organizations may find it more cost-effective to distribute these duties across existing positions. However, the assignment should be a specific line item in the relevant job descriptions. Surrounding policies and practices must be consistent with the assignment. That is, the responsible party should have adequate authority and resources. Performance evaluations, merit raises, and so on must take into account control performance.

For any size entity, explicit assignment of control responsibilities will likely mean a consolidation of some functions and personnel and the addition of some incremental staff and activities. Rationality would dictate that these incremental costs be weighed against the reduction in risk they would buy. But these changes are fundamental. They serve to reduce almost every type of data processing exposure an organization may face, rather than eliminating or reducing a specific few. Thus the benefits are often almost impossible to measure, and the amount of incremental resources must be something of a judgment call.

(3) Life-Cycle Methods and Other Standards. Many companies do employ design and/or programming methods or standards to guide in-house application development. We do not mean to denigrate these efforts. However, much more is needed. Figure 8 illustrates how risks permeate every phase of the system life cycle. And by no means are all services supplied from a central in-house

department, especially in larger organizations. Comprehensive control requires policies, standards, and procedures for every phase of the life cycle from problem identification through eventual application retirement, and for all data processing use, whoever provides the resources.

A company may develop its own systems life cycle guidelines or purchase such a program from a supplier. In either case, care should be exercised to assure that neither the peculiarities of the company's requirements nor the universal characteristics of data processing systems are neglected. The costs associated with selecting the wrong methodology are possibly greater than the costs of not selecting any.

If a commercial method is selected, it likely will require modifications to adapt it to the unique requirements of the company. The methodology must not be an unnecessary burden, or significant efforts will be made to circumvent the control it represents. Should the organization choose to develop its own standards, it can benefit greatly from reviewing commercial methods, and those developed by other companies.

Standards alone are not enough, however. Someone must be responsible for their day-to-day administration, including the granting of reasonable exceptions to them. This role easily falls to the aforementioned Control Director. Also, someone must from time to time monitor (audit) the application of these standards. This task logically belongs to internal or external auditors. Whomever these responsibilities fall to, they must be explicitly included in the life-cycle program.

(4) The Provision of Adequate Resources. Properly controlled systems appear to cost more to install and operate--but only when one fails to include the probable cost of breakdowns due to lack of such controls. Unfortunately, the potential cost of breakdowns may be difficult to estimate. Even data

Examples of Life Cycle Risks

Figure 8

In Problem Analysis

Problem is incorrectly or incompletely specified
Problem is assigned an inappropriate priority

In Procurement

Inadequate hardware or software selected
Budgets overrun
More cost-effective solution overlooked

In Development

Design is incorrect or incomplete
Programming does not conform to specifications
Inadequate documentation for operation and maintenance
Budgets or time schedules overrun
Fraudulent use incorporated in system

In Operation

Data entry errors
Processing errors
Hardware failures
Operator errors
Natural catastrophe

In Maintenance/Modification

Unauthorized/fraudulent programming changes
Authorized changes are not made, or are installed incorrectly
Programs cannot be maintained due to loss of key personnel or lack of documentation
Necessary changes are not identified or cannot be implemented

processing professionals admit having trouble identifying all the breakdowns that could occur. Even if risks can be identified, the likelihood of their occurrence and/or the costs if they did occur may prove difficult to determine. Thus, there is often no quantitative measurement of risk reduction associated with a given control. So we cannot prove that incremental resources would be cost effective. We can only note that until very recently, the whole issue of data processing risks and controls has been ignored, and that probably means that at least some incremental investment is justified.

With the explicit assignment of control responsibilities added to current duties, existing personnel may become overburdened. Additional personnel will probably be required to cover the new control duties adequately without compromising other activities. Back-up facilities, off-site data storage, fire protection, access control, uninterruptable power--all these obviously cost money. We do not mean to imply you need all these things, but we suspect you may need some.

Controlled software utilizes more computer resources in operation than uncontrolled systems. Input validation, production of audit trails and error logs, program back-up, charge-back billings, and many other control techniques use CPU and peripheral resources. It takes more time to develop properly controlled systems. Risk evaluation and control design are added to the development process. More code must be written than if input-process-output control were ignored. Controlled systems take longer to document. And so on.

It's that old saw: there's no such thing as a free lunch. Think of it as insurance--the principles are much the same. Insuring your house costs more than not insuring it--unless you suffer a fire, flood, theft, or other damage. Then the insurance looks cheap.