Woman C.P.A.

Volume 48 | Issue 4 Article 3

10-1986

Managing PC Growth: Guidelines for Good internal Control

Phillip W. Balsmeier

Angela Letourneau

Managing PC Growth

Guidelines for Good Internal Control

By Phillip W. Balsmeier and Angela Letourneau

Audit Objectives

The objectives of electronic data processing (EDP) auditing are to safeguard assets, maintain data integrity, achieve organizational goals effectively, and consume resources efficiently [Weber, 1982]. These objectives form a framework within which the growth of PCs should be evaluated. PCs started out with limited capacity to manipulate small amounts of data, but technology quickly produced free-standing machines with sophisticated capability to manipulate megabytes of data.

The next step in the computer revolution, networking, will exponentially increase the amount of data available from a PC workstation. The PC will be capable of accessing the entire company data base, combining the benefits of a mainframe operation with the convenience of the PC workstation [Snow, 1985b]. The benefits to be enjoyed from this technological step forward are obvious, but the need for comprehensive controls has been largely overlooked. Proper controls will provide the capability necessary to perform authorized operations while limiting the dangers of too much access.

The attendant problems are much the same as when the mainframe computer was first introduced: control over data entry, data pollution, and data misappropriation. The difference now is that the number of people potentially involved has mushroomed. Survey results .published by Schultz [1985a] revealed that 89 percent of firms used micro computers in their organizations. The time is arriving when every employee will have access to some part of the data base. Corporate policies, computer procedures, and computer software capabilities should converge upon a solution that will allow the convenience of the personal computer while not compromising the integrity of the data base.

Corporate Policy

Guidelines on the use, growth, and application of PC systems should come from high level management. Romney and Stocks [1985] identified that controls for PC acquisition start with a formalized company plan. The plan should specifically address the expected uses of microcomputers and how such uses would benefit the firm. A cost/benefit analysis, the company competitive status, and the time and money required to adapt to the expected work environment also need to be considered. Vendors or consultants may be contacted for their input. This is a better approach than buying a PC because everyone else has one and then seeing if it can do anything useful for the organization.

Formal corporate policies are essential to the orderly development of data systems. One individual should be assigned the primary responsibility of establishing an information center to oversee all pertinent PC issues [Romney and Stocks, 1985]. Such a person may also head a PC steering committee or clearing authority that coordinates all purchases of hardware and software. Snow [1985a] suggests that the information center would establish software libraries and oversee internal seminars and other training, as well as take responsibility for security and backup procedures. The information center should also plan PC system implementation, customize PC software, and train personnel.

The information center should be the backbone of corporate policy. Based on their survey results, Schultz and Redding [1985b] reported that 15 percent of companies with PCs had no policy enforced. In only 5 percent of companies surveyed were purchase requests reviewed and the purchase negotiated by the EDP department. Only 6 percent had company specifications enforced. Many other weaknesses were evident in the procedures designed to implement company policies in the firms surveyed.

A number of situations contribute to the fact that there is often no corporate policy to control the growth of PCs within a company. One is the fact that software and personal computers are relatively cheap; therefore, many people within the organization are authorized to make purchases within the cost parameters of the small systems. Many of these people know little about computer systems and are at the mercy of vendors. Understandably, a company often ends up with several incompatible brands of equipment.

Sobol [1985] reported that some companies have set up in-house computer stores that allow employees to inspect a variety of computer products to determine which would best fulfill their needs. The store can provide both choice and compatibility and can be an important step in the direction of standardization of hardware and software within the company. The central clearinghouse concept is an excellent means of establishing positive control over the PC inventory at the time of purchase. Another facet of good management control sustained by the clearinghouse concept is proper support and training. Standardizing the types of equipment and software used simplifies the initial training, reduces the amount of necessary retraining when there are interdepartmental moves, and reduces the variety of in-house maintenance support required.

Procedures

The second phase in bringing the PCs under control is to establish procedures to protect the data base. An initial step would be to determine how dependent the firm is on its computerized information system. Dascher and Harmon [1984] state that the firm must consider how dependent it is on the computer for day-to-day operations, how much data is computerized, and how critical the data is to the success of the firm. If company personnel need frequent access to computerized records to service clients, then the firm is computer dependent. A relatively large amount of computerized data will usually make a firm vulnerable. Data sensitivity is also very important. A firm needs to consider how much damage would occur if sensitive information, such as sales or production data, got into the wrong hands.

The time is arriving when every employee will have access to some part of the data base.

With a firm understanding of the company's risk, the existing controls can be evaluated. The main categories of control are physical, operating, access, and personnel. The idea is to match exposure to risk with the proper level of controls. If an inspection reveals areas of low risk and costly controls, a reduction of controls, and therefore of cost, would be appropriate [Dascher and Harmon, 1984].

Guidelines established for mainframe operations are very applicable to PCs. A full set of basic measures would include diskette security, password access controls, proper program development, and backup procedures. Common application controls such as hash totals, run-to-run totals, and record counts are also as appropriate to PCs as they are to mainframe operations.

The direction in which PC usage is moving and its accompanying security threat provide a classic confrontation between progress and security. Already there are firms planning to provide a PC for every worker, striving to derive the ultimate benefits from data access, continuously updated information, interoffice communication, immediate customer servicing, and other sound business goals. But the implied unlimited access to information is a nightmare of data security threats. Without controls, there is great potential for changing programs to the advantage of an employee, altering data to cover up errors or misappropriations, selling of sensitive information to competitors, and stealing of hardware.

Security measures take away some of the benefits derived from PCs. For instance, to prevent theft, the units could be secured to a desk, but that removes the advantage of PC portability. Nevertheless, some security measures should be implemented.

Diskette protection is a major problem. Security measures to protect against theft of files on diskettes are weak. Downloading of information onto a diskette and carrying the diskette out the door is a simple matter. One aid to security is a disk with a unique "fingerprint" or "signature" [Romney and Stocks, 1985]. If the fingerprint is not found, the program is not executed. Additional protection in this area will require changes in system software design.

Several other data protection measures may be considered. To protect against vandalism or other loss of data, backup files should be kept in a secured area. Locked computer workrooms would provide some security but seriously reduce the convenience of PCs. PC physical security is a serious problem, and there are few alternatives at hand beyond the inadequate and simplistic lock and key.

In the case where data leaves the office by telephone line, Haigh [1985] advises the use of data encryption to protect highly sensitive data. For less sensitive data, many companies use a callback scheme. When access to data is requested, the program detects a special code transmitted by the user's modem and calls back when the number is verified.

Password protection and access controls are two powerful methods of protecting data from excessive error pollution, destruction, and theft. Access controls offer a variety of safety measures. First, access to particular files can be restricted to those who have need for access. Order clerks, for instance, have no need for access to payroll files. Secondly, access controls can subdivide those with access into those who can view, copy, and/or change the data. Access can be limited to one or more specific machines, to those with a special entry code, or both. Passwords and access controls are generally used in tandem; an individual needs a password to have any access and an access control to get to specific files.

Romney and Stocks [1985] suggest the use of an authorization table as an access control. The table has a profile of each user and the procedures or data to which he has access. If an unauthorized entry is attempted, the request is denied. Some such systems will record information on unauthorized attempts and make the record available for supervisors to review. Personal data checking can also be used as an access control. Haigh [1985] indicated that techniques such as the use of voiceprints to authorize access are only in limited use now but hold promise for the future.

A major problem with both passwords and access controls is the security of the words themselves. If the words are taped to the computer screen, the control is defeated. So along with the procedure, there must be education of the workforce, constant monitoring of the procedure, and strict enforcement of the rules. The codes must be changed periodically, and the master list of passwords tightly secured.

Job rotation on a nonsystematic basis is another control technique. The longer a person is left at one job, the more capable he or she is of subverting the system. If the company staff is too small to support wholesale job rotation, the cross-training of personnel should be considered. Cross-training is a good procedure in any case.

Proper controls will provide the capability necessary to perform authorized operations while limiting the dangers of too much access.

The means of protecting the integrity of the data bases are available. There is no gap in technology preventing good security, only lax management. The problems inherent in software protection, on the other hand, comprise elements of both technological and managerial weakness.

Software

The primary recommendation in the area of software is that EDP auditors, or whoever fulfills that function, should be responsible for, and be heavily involved in, the development of security controls [Snow, 1985a]. This is a traditional responsibility of EDP auditors, but one that they have not always been allowed to perform. Schultz and Redding [1985] stated that the importance of the involvement of EDP auditors will increase tremendously as the sophistication of the PC grows.

The complexity of software controls is evidenced by a recent study by the University of Georgia. A questionnaire was sent to 500 internal and external auditors and to systems personnel. They identified 59 control items as a set of "minimum EDP controls that should be included by a vendor in a turnkey . . . accounting system," [Stivers, 1985]. The sheer number of controls, plus the fact that they are accounting controls for the purpose of facilitating the jobs of auditors, points out the critical need to have the EDP auditor deeply involved in the development of new programs and the alteration of old programs at the inception of these procedures.

Stivers [1985] indicates that one of the reasons the controls have not been included in the past is that many users were unaware of the need for them, and the CPUs of the early machines did not have the necessary capacity to store numerous controls. Controls cost money, and in the competitive environment of software vendors, it was beneficial to keep the cost as low as possible.

Promulgation of the 59 recommended controls is an attempt to influence software vendors to produce a product that will meet the needs of sophisticated users. The recommendations also attempt to establish some minimum industry standard. Vendors can be expected to respond only if there is a strong demand from business for such products. To generate the required demand, high level management must be made more aware of the value of a secure and error-free data base and understand that the information in the data base is often a firm's most important asset.

The idea is to match exposure risk with the proper level of controls.

The safeguards put in place by management are the best protection against costly reconstruction of records and theft. One retailer estimated that the cost of reconstructing 25,000 accounts would be 1.4 million dollars [Menkus, 1985]. Management must not rely on prosecution as protection against theft because theft of information is difficult to prove. In many cases, proof is required that records were actually removed. Most often, in the case of computer records, the information is copied, but the records are not removed. Computer software currently sold by vendors is primarily designed to be user friendly, not secure. Normally the software lacks controls, data is easily destroyed, and documentation is weak [Stivers, 1985].

As PCs become more sophisticated and users become more knowledgeable, the current caliber of software may fall from favor. Software vendors can anticipate this evolution and benefit themselves and their customers. The focus should be on the design of the software. Structured design should be used in developing the program, and there should be independent testing of the controls and aids before the product is put on the market.

To protect a company's capability to modify software should the vendor go out of business, the company may arrange to have a copy of the source code available rather than only the executable machine language copy. Most vendors will not release their source codes, but they may agree to have one put into the hands of an independent third party. This escrow copy would be used only if the vendor could not fulfill his obligations to the buyer [Sobol, 1985].

PC program development within the firm requires internal control. Every change to a program must be subject to program code peer review to assure that the change will operate as intended and be within the security guidelines. In addition, each program and program change should be fully documented. There should be a complete and readable reference source with instructions sufficiently clear as to allow someone unfamiliar with the program to obtain the desired results [Snow, 1985b]. The firm could suffer serious delay

Phillip W. Balsmeier, Ph.D., *is an associate professor of management at Louisiana Tech University. He received his Ph.D. from the University of Arkansas. His articles have appeared in various journals.*

Angela Letourneau, CPA, MBA, *is a doctoral candidate and instructor at Louisiana Tech University. She is a former internal revenue agent in the examination division.*

or expense if one key employee who understood the program were incapacitated or left the firm.

Software development should be monitored by the central control group. This will not only assure the viability of each proposed program, but also reduce redundancy among programs and help assure that each user is taking full advantage of existing programs [Timko, 1983]. By minimizing the number of programs in use, storage, training, and documentation, costs will also be reduced and profits enhanced.

Summary

The general plan for controlling the growth of PCs within a firm is in line with the goals of EDP auditing. Management control of PC expansion, along with the involvement of EDP auditors in software development, will help assure that organizational PC goals are achieved effectively. The clearinghouse concept enhances the efficient use of resources, and protective measures help safeguard assets and maintain data integrity. Ω

REFERENCES

Dascher, Paul E. and W. Ken Harmon, "Assessing Microcomputer Risks and Controls for Clients." *The CPA Journal,* May, 1984, pp. 36-41.

Haigh, Peter J. "Microcomputers and the Man With the Red Flag." *The EDP Auditor Journal,* 1985, Vol. I, pp. 13-21.

Menkus, Belden. "Protecting Corporate Data." *Journal of Systems Management,* April, 1985, pp. 14-19.

Romney, Marshall B. and Kevin D. Stocks, "Microcomputer Controls." *The Internal Auditor,* June, 1985, pp. 19-22.

Schultz, Norman O. "Microcomputer Control Strategy: An Empirical Study of Its Development." *The EDP Auditor Journal,* 1985a, Vol. I, pp. 1-12.

__________ and Rodney J. Redding. "A Survey of Microcomputer Control and Support Policies." *The EDP Auditor Journal,* 1985b, Vol. II, pp. 5-19.

Sobol, Michael. "Microcomputers & Auditing Don't Make the Same Mistake Four Times." *The EDP Auditor Journal,* 1985, Vol. I, pp. 37-41.

Snow, Martin A. "Auditing Microcomputer-Based Application Systems." *The EDP Auditor Journal,* 1985, Vol. I, pp. 25-35.

__________. "Taming the Micro Revolution: The Need For Policy." *The EDP Auditor Journal,* 1985, Vol. II, pp. 1-4.

Stivers, Bonnie B. "Internal Controls for Small Business Computer Accounting Systems." *The EDP Auditor Journal,* 1985, Vol. II, pp. 20-28.

Timko, Ronald J. "Controlling Microcomputers — Don't Overreact." *The Internal Auditor,* December, 1983, pp. 20-22.

Weber, Ron. *EDP Auditing Conceptual Foundations and Practice.* New York: McGraw-Hill, 1982.