ACCESS AND COMMUNICATION CONTROLS
IN AN ACCOUNTING INFORMATION SYSTEM

by Avi Rushinek and Sara F. Rushinek

University of Miami,
Coral Gables, Florida

Abstract

This paper involves the exploration of two very important security controls in a computerized accounting information system: (1) access controls, and (2) communication controls. The various specific access and communication controls are examined, analyzing their roles in an accounting information system's computer network.

The growing use of computers in the accounting information systems of the business environment, along with the presence of growing computer fraud, necessitate managements to implement stricter access and communication controls.

Introduction

Used in the broadest sense, "controls" are methods and/or procedures used by and within an organization to safeguard its assets. The importance of controls in an Accounting Information System (AIS) or the Electronic Data Processing (EDP) System is both prudent and understandable when one considers the following factors: First, an automated AIS is likely to process more data than the manual one -- increasing the number of both potential errors and potential problems. Computerized AISs also gather, process, and store data in non-readable (by the human eye) forms, thus eliminating the possibility of observation to check for data accuracy and integrity. The audit trail has also been blurred in the use of AISs due to its nature of taking one system entry and sending it simultaneously to several different places in the entire system, according to Moscove and Simkin (1981). Other control considerations, or the need for them would be: (1) Management has come to rely increasingly on computer generated reports, and many major financial decisions are made on the basis of these reports. (2) Tremendous amounts (if not all) of a company's resources are controlled by AISs and/or EDP systems.

Analysis, Synthesis and Discussion

Some of the primary objectives of controls are: (a) to insure that transactions are processed in accordance with management's authorization; (b) to insure that transactions are processed and recorded properly; (c) to insure that transactions which are not processed or recorded correctly, or transactions which are not processed in accordance with management's authorization are detected; and (d) improper transactions that are detected are corrected to the extent possible, as stated by Harrison (1981).

Exposures are risks or threats that an organization is subjected to. Controls should seek to prevent, eliminate, and/or minimize costs and problems associated with exposures. Any action leading to an exposure is known as a cause of the exposure. A good control system will reduce, minimize, or preclude some of the more typical exposures such as: (1) destruction or loss of assets; (2) interruption of business; (3) bad management decisions; (4) unreliable record keeping; (5) unreliable data; and (6) possible competitive disadvantage. There are three categories of exposure reduction/control. The first category is that of Preventative - which (hopefully) keeps the cause or causes of exposure from occurring. The second set of controls falls under the heading of Detective Controls. Once a cause of exposure has taken place, this type of control has then to detect it. Thirdly, Corrective Controls present and provide information needed to determine the causes of exposures and the corrections of them, as discussed by Harrison (1981).

Summary, Conclusions and Implications

This paper reports on two important areas of control concerning computer usage in an accounting information system: (1) access controls, and (2) communication controls. Both sets of controls encompass a vast array of subset controls, each equally as vital as the next.

© 1983 ACM 0-89791-113-X/83/0010/0119$00.75

Access and communication controls are designed to: (1) insure that transactions are processed in accordance with management's authorization; (2) insure that transactions are processed and recorded properly; (3) insure that transactions which are not processed or recorded correctly, or transactions which are not processed in accordance with management's authorization are detected; and (4) insure that improper transactions that are detected are corrected to the extent possible. The various access and communications controls were examined, and each of their advantages and disadvantages were analyzed.

The implications of this research is fairly clear. With the growing use of computers in the accounting information systems of the business world, coupled with the corresponding growth of computer crimes being prepetuated not only by "outsiders", but also by intelligent (though misguided perhpas) employees; management must give strict attention to the necessary and applicable access and communication controls available for implementation in their computerized accounting information system. Adherence to this advice can save millions of dollars of a company's most important or valuable resources, which in turn, can be invested toward the advancement of a company's computer technology.

References

Available upon request.