COMPUTER CONTROL AND AUDIT

THE INSTITUTE OF INTERNAL AUDITORS

COMPUTER CONTROL & AUDIT

by
William C. Mair, CDP, CPA
Detroit, Michigan
Donald R. Wood, CPA
Chicago, Illinois
Keagle W. Davis, CPA
Minneapolis, Minnesota
Partners
TOUCHE ROSS & CO.

Published and distributed by The Institute of Internal Auditors, Inc., 249 Maitland Ave., P.O. Box 1119, Altamonte Springs, Florida 32701, with the permission of the copyright owner, Touche Ross & Co.

ISBN 0-89413-063-3

Foreword

The computer has been described as a dominant advance of the 20th Century. Certainly it is a primary reason for the accelerating evolution of business methods. Applications are no longer computerized simply to gain the benefit of the speed and reliability of automated equipment but to use a new approach in performing applications.

The advent of electronic funds transfer systems, on-line data bases, and networks of interconnected computers provides management with new challenges which have created new problems. For one thing, the traditional methods used to control organizations in a manual environment are not effective in a computerized business environment. New control techniques are needed to be responsive to and complement the characteristics of the computer.

These changes are reflected in the problems auditors have in evaluating the reliability of computerized applications. Without established internal control mechanisms, auditors are turning to external measures to control computerized applications. This is because data processing personnel have not spent enough time evaluating computer-generated exposures and risks to their organizations or developing adequate internal control systems for monitoring computer functions. Weaknesses are particularly evident where manual and computerized portions of an application interface.

Computer Control & Audit by Mair, Wood, and Davis of Touche Ross & Co. addresses these problems. The prerequisite to effective auditing is effective control. This book discusses controls from a preventive, detective, and corrective viewpoint. The objective of controls, to reduce exposures, is discussed in detail together with practical methods of improving controls in data processing applications.

Written by practitioners who worked in conjunction with many large corporations to present practical data processing control concepts from the viewpoint of control-oriented personnel, the book is a valuable addition to the personal library of data processing systems analysts and managers as well as auditors. For the first time, control is adequately explained from an accountant's and auditor's viewpoint. The book answers the key question: Why is the total system of control over data processing applications a major concern of data processors? In answering this question, the authors take a practical and logical approach to the analysis of all varieties of controls used in computerized and manual information systems.

Ruth Davis
Deputy Director (Research and Advanced Technology)
Office of the U.S. Director of Defense, Research, and Engineering

Preface

Recognizing the need to provide auditors with information on the audit and control of computer systems, The Institute of Internal Auditors issued a manual entitled *Internal Auditing of EDP Systems* in 1968. This book helped innumerable audit groups to establish the EDP audit function and to become involved in the audit and control of computer applications.

IIA's International Research Committee recognized in the early 1970's that *Internal Auditing of EDP Systems* was becoming outdated and that it would have to be replaced. The committee's recommendation was to amplify an existing book published in 1972 by Touche Ross & Co. with the same title as this volume. The International Research Committee formed a task force under the direction of Robert Logue of the 3M Company to work with Touche Ross' authors of the original book. The objective of the task force was to supplement the book with the viewpoints of internal auditors, top management, and data processing personnel and, at the same time, to update the book to reflect current technology. The result was the publication of this book.

This comprehensive manual on computer audit and control outlines a methodology for evaluating the process of internal controls in computer systems. To date, most auditing literature has alluded to the process of evaluating controls without defining this process. It is not intuitively obvious to many auditors what is meant by adequate control in data processing. A prime objective of this manual is to help answer that question. The manual is developed from actual field experience by practicing internal auditors and certified public accountants.

The Institute is deeply indebted to the authors of this book: William Mair, CPA; Don Wood, CPA; and Keagle Davis, CPA. We are also very grateful to Touche Ross & Co. for having donated this book to The Institute.

This book represents the diligent efforts of numerous individuals, and The Institute of Internal Auditors expresses its appreciation to all those who made this manual possible.

John D. Bradt, CIA
International President
1975-1976

THE INSTITUTE OF INTERNAL AUDITORS
INTERNATIONAL RESEARCH COMMITTEE
1976-1977

Frank F. George, CIA, Chairman
Norton Company
Worcester, Massachusetts

Grady Adair, CIA
General Telephone Co. of Fla.
Tampa, Florida

Robert L. Adams, CIA
Aetna Life & Casualty
Hartford, Connecticut

William C. Anderson, CIA
Continental Illinois National
Bank and Trust Co. of Chicago
Chicago, Illinois

Archie J. Bakay
Mansfield, Ohio

Jack A. Boggs, CIA
South Carolina National Bank
Columbia, South Carolina

Edmund N. Carlson, CIA
University of California
Los Angeles, California

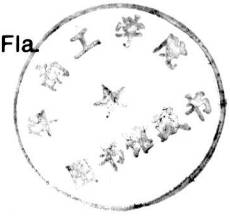
W. F. R. Evans
Standard Telephones & Cables Ltd.
London, England

C. W. Gissel
Thiokol Corp.
Newtown, Pennsylvania

Paul E. Heeschen, CIA
Lockheed-California Co.
Burbank, California

Gilbert C. Hogue, CIA
Western Electric Co., Inc.
Indianapolis, Indiana

Elmer R. Kramber, CIA
Western Air Lines, Inc.
Los Angeles, California



Robert P. Logue, CIA
3M Company
St. Paul, Minnesota

Alan T. McCleery, CIA
North American Rockwell Corp.
Downey, California

Clifford M. Nugent, CIA
Mesa Public Schools
Mesa, Arizona

James W. Pattillo
University of Notre Dame
Notre Dame, Indiana

James H. Reber, CIA
Sperry New Holland
Zedelgem, Belgium

John Reeve, CIA
Clinch River Breeder Reactor Project
Oak Ridge, Tennessee

William H. Sachau, CIA
Tulsa, Oklahoma

William E. Thompson, CIA
Alabama Bancorp.
Birmingham, Alabama

Donald J. Whittingham, Jr.
Warner & Swasey Co.
New Philadelphia, Ohio

William D. Worrell, CIA
Omaha, Nebraska

Robert J. Symon
Bache & Company, Inc.
New York, New York

William E. Perry, CIA, Director
Professional Practices Department
The Institute of Internal Auditors
Orlando, Florida

Acknowledgments

We are deeply indebted to a large number of individuals whose advice and assistance were essential in writing this book.

The following members of Touche Ross & Co. directly contributed their ideas and enthusiasm to the contents:

Paul Hamman, CPA
Hugh Hardie, CA
John Lehman, CPA
James Loebbecke, CPA
Carl Pabst, CPA
Richard Webb, CPA

Advice, review, and editing were provided by an IIA committee of reviewers that included:

Willard E. Hick, III
Massachusetts Mutual Life Insurance Company
Robert P. Logue, CIA, CPA
3M Company
Frederick B. Palmer, CIA
Chairman, International EDP Audit Committee,
Institute of Internal Auditors
Raymond S. Perry
Xerox Corporation
William E. Perry, CIA, CPA
The Institute of Internal Auditors

In addition to these individuals, who are easy to identify, we must offer our thanks also to a multitude of associates whose efforts and experience developed the accumulation of knowledge related herein. A list of these individuals would be so vast that space does not permit it here.

Finally, we would like to thank Brenda Walton for her extensive labors in preparing the manuscript.

William C. Mair
Donald R. Wood
Keagle W. Davis

Prologue

Why should computer controls be of concern to businessmen? Should auditors give them special attention?

The Equity Funding fraud, for all of the millions of dollars that it cost investors, is somewhat facetiously credited for providing the greatest contribution in recent years to the goal of strong computer controls. The authors' accounting firm was engaged by the bankruptcy court to produce more realistic financial statements after the discovery of the fraud. Although the press credited the success of the fraud to the sophisticated use of computers, we found, rather, that only 19% of the fictitious assets claimed by Equity Funding had any relation to the use of computers. In fact, most of the assets were wholly without any type of support by computer or anything else. The only role that a computer actually played was to create some rather weak support for certain fictitious insurance policies that Equity Funding was selling to legitimate insurance companies.[1] If Equity Funding were all we had to worry about regarding computer fraud, we wouldn't really have much to worry about.

The opportunity for computer fraud that should cause greater concern is the programmer's ability to manipulate the computer as though it were a puppet. He does not need to have direct access to the actual computer equipment. By submitting programs with subtly imbedded routines to perpetrate a fraud or evade existing controls, he may gain control of huge quantities of assets.

A case of programmed computer fraud occurred in a revolving-credit-card system. A programmer provided a little "extra" maintenance along with some routine program changes. Thereafter, on the tenth day of each month, the first $100 payment processed was credited to the programmer's own account. The second $100 payment was credited to the account of the first payment, and so on. A complaint resulting from the eventual shortage in the last account could never be traced to the programmer. The programmer never came near the computer room.

In spite of these examples, relatively few cases of computer fraud or embezzlement are uncovered — particularly when one considers the number of opportunities that exist. Based upon our obser-

---

[1] *Report of the Trustee of Equity Funding Corporation of America Pursuant to Section 167(3) of The Bankruptcy Act [11 U.S.C. §567(3)]* by Robert M. Loeffler. Trustee United States District Court Central District of California, February 22, 1974, p. 38 and October 31, 1974, pp. 137-139.

vations, relatively few companies have sufficient internal controls to reliably prevent or detect acts of computer fraud and embezzlement. Apparently, the only reason computer fraud and embezzlement are not more common is that data processing personnel are generally honest. In comparison to the other problems that exist, the exposures to computer fraud and embezzlement seem to be relatively minor. This is not to say that they are negligible but, rather, that other and more substantial problems should command the greater concern and attention.

The business records maintained today on a computer may constitute virtual "information assets" of the organization. Although not negotiable, these assets may even be more critical to the successful operation of the business. If they are damaged or destroyed, they may threaten the very existence of the business enterprise.

Probably the greatest threat to these assets, like their more tangible cousins, is fire. The computer equipment and machine-readable records can be damaged by temperatures as low as 120° F. While fire seldom occurs within computer equipment, fire in an adjacent area may easily spread.

A computer manufacturer experienced a serious fire in a computer center used to distribute software products. The fire started in the basement used to store packing materials for the shipment of the software products. The intensity of the heat structurally damaged the computer room floor on the level above and entered the computer room via conduits provided for electrical cables. Water used to extinguish the fire added to the destruction. Millions of dollars of computer hardware and information assets were destroyed.

What makes the risk from catastrophes greater with computers is the totally new level of concentration of information assets that they promote. The comparison of information assets between a paper environment and a computerized one is like comparing a cash register to a bank vault. The consequent effects on risk management may be compared to an insurance company having all of its policies on buildings within a single block. Although the probability of destruction is not increased, the potential consequences certainly are.

The risks provided by this concentration of assets do not involve only the catastrophic destruction. Daily operating errors may also have massive consequences.

The computer operator in a medical institution forgot to remove the "protect ring" on a magnetic tape that constituted the sole record of approximately $.5 million in cash receipts. He accidentally mounted the tape on the wrong tape drive, and it was erased. As a result, past-due receivables could not be identified and pursued. To assist in the reconstruction, additional labor had to be hired. About the time that the reconstruction was finally complete, the same accident happened again.

Computer records often play an essential role in the business information systems. A serious deficiency in the quality of these records or their complete loss can cause "organizational amnesia." This occurs when the business information system fails to provide accurate and timely information regarding the activities of the organization. As businesses grow and must deal with an increasingly complex society, the effects of organizational amnesia become of greater concern. Businessmen must take positive steps to assure that their survival is not threatened.

A small aerospace manufacturing company developed a high-technology consumer product having great appeal. Within two years it grew from a business that serviced only 20 customers to a household name selling directly to more than 15,000 retail establishments. However, its information system for the collection of receivables was completely inadequate to control the growth. Three years after its successful product introduction, the company declared bankruptcy — a victim of organizational amnesia.

While serious threats, catastrophe and organizational amnesia are still not the primary reason for concern with modern computer systems. Fires do not occur every day; and many businesses can continue to exist, even though their internal information is limited or inaccurate.

Based on our experience, *the greatest sources of computer losses are innocent errors and omissions.* Users may be excluded from development and operation of computer applications and, therefore, never really understand the meaning of the information they receive nor the role they play in controlling it.

A receivables application included excellent controls: starting when the data entered the computer room and ending when the reports left it. Since a computer produced the reports, they were regarded as infallible. Auditors soon discovered, rather, that customer payments were so hopelessly misapplied that they could only request that the customers inform the company of the amounts owed per their records. The company eventually went out of business.

Although computers are highly reliable at what they do, they only do that which is programmed and, then, only with information that is provided from humans. Errors and inaccuracies in these inputs may be the source of millions of dollars of losses.

A medical institution developed a sophisticated computer system to gain better control over patient billings and collections. One major feature of this system was an error suspense file that controlled follow-up on items submitted with apparently erroneous information. The system provided capacity to control 100,000 error items in suspense at any time. Within three months after inauguration of the system, this file contained 120,000 items and was completely out of control. No one had ever dreamt that the volume of

erroneous information being submitted could be so massive. Auditors had to be called in to institute computer-assisted auditing techniques to resolve most of the exception items.

Even one error in certain types of inputs can have a persistent, recurring effect.

A large wholesaler was forced to raise prices in order to recover inflationary increases in costs. However, the "new" price list that was fed into the invoicing system was actually the list of six months previous. Incorrect billings were issued for two months for a loss of $80,000. Recovery efforts cost another $20,000 for a total of $100,000.

Computers lack the tolerance for erroneous inputs that manual systems previously could handle. Clerks who operated manual information systems would often recognize ridiculous situations and correct them without hesitation.

A manufacturing company converted its inventory control system from a manual system to a computerized one. They were pleasantly surprised but somewhat perplexed when the reported inventory increased by approximately $1 million. Subsequent investigation eventually disclosed that the instruction manuals for their product were classified under the same part number as the machine they described. The 50 manuals in stock were treated by the computer as also being worth $20,000 apiece.

Even when proper inputs are provided to computers, they can still produce absurd results.

Depreciation calculations of an aerospace company contained assets with a negative net book value. Although the programming staff was instructed regarding the various acceptable depreciation methods, none of the finance people had ever informed them that depreciation calculations stop when the net book value reaches zero.

Logic problems in computer processing do not simply evolve from any natural process. They are caused! The vast majority of the cases are caused by poor or nonexistent communications between the data processing personnel and the other members of the business organization. However, even perfect communications will not eliminate all problems.

In a financial institution, the interest calculation on savings accounts was erroneously programmed as if there were 31 days in every month. In the five months before it was discovered, over $100,000 in excess interest was paid out.

The error rate in programmed functions is intolerably high. Even "tried-and-true" applications may contain subtle defects that exist for years.

A large retail establishment computed its aging of receivables incorrectly for three years before it was detected. It was impossible to determine what effect this had on its collections of receivables.

Experienced EDP auditors may expect to encounter programmed errors in 30% of the applications they test. This percentage is lower among financial institutions and higher in manufacturing and service organizations. Rates of as high as 60% have been observed. Fortunately, the majority of the errors that are detected do not have material financial consequences. On the other hand, some of them amount to millions of dollars.

Another financial institution was making discounted installment loans. Upon receiving the information of the amount of discount, the computer would calculate the effective yield on the loan and store that yield for use in subsequent interest-earned calculations. Unfortunately, the programmers did not allow the system to accept any discount values of $1,000 or more so that, when such amounts were occasionally submitted, they would be truncated and produce a lower apparent yield than the actual loan. By the time this was discovered by the auditors, misstatements in earnings had already accumulated to $1.5 million; and more than $.5 million had already been allowed in excess rebates to individuals who repaid loans early.

Approximately five percent of the items carried by a company in the distribution industry were so-called "catalog items" whose unit cost was based upon the volume purchased in a year. The company's rule was that inventory items would be valued at the lowest amount of such sliding-scale prices representing the highest possible purchase volume. Prices paid in excess of the minimum would be expensed as variances from standard. A minor error in the logic of valuing inventory reversed this rule, however, and valued these items at the maximum price or minimum quantity. The effect was to increase the reported value of inventory by approximately $10 million.

Not only do the applications being developed contain numerous subtle and not-so-subtle errors, but they also cost far more to develop than ever intended. One popular seminar on EDP controls presents materials stating that cost overruns in the development of computer applications of 250% are "typical."

There is a tremendous need for better controls designed more economically and reliably. Systems design personnel may be trained in "systems analysis" but rarely are trained in the design of controls. Many controls that they institute are not even recognized as controls. They are just the way things are done . . . sometimes. Auditors, who are supposed to be the control experts, will list off numerous controls that they think should be provided but rarely provide any explanation as to *how* they reach their conclusions. As a result, the systems designers repeat the same errors and omissions with the next system.

The data processing personnel of a large mail-order house designed a "perfect system." It would only operate if everything else worked perfectly. After implementation, the auditors discovered that

errors were occurring at the rate of almost 50 percent. The system swiftly collapsed and had to be abandoned after investment of approximately a quarter of a million dollars.

In spite of the absurd results they occasionally produce, computers have come to be considered an essential part of the business environment. At the end of 1973, 133,000 computers valued at almost $30 billion were in use. The number of installed computers will grow to 500,000 by 1978 with a projected value of over $50 billion. The reason for the increase in value being less than proportionate to the number of units is because the heaviest growth is taking place in the very small units, although a heavier rate of growth is also noted in the very large machines.[2] Given this phenomenal growth, we must ask what need are these machines satisfying?

A medium-sized company in a service industry installed a medium-sized computer for which the rent was approximately $100,000 per year. When their utilization was evaluated, it was found that the machine was being used only 22 hours per month. The equipment had obviously been installed based upon the management's desire to appear progressive and modern rather than any economic evaluation of the actual needs.

In spite of the horror stories on things that go wrong with computers, some systems are designed and function properly.

A service organization designed a "cradle-to-grave" automated accounting system. Their design methodology followed a textbook approach precisely and was performed by trained and expert systems personnel. After careful design for more than seven man-years, the system was implemented and has now been operating for five years with an almost perfect record for reliability and accuracy.

Strong, well-directed management is what makes the difference. Data processing management is a very new profession. Business applications of computers only reached a wide scale in the early 1960's. Current standards for effective EDP management may be quite unfamiliar to individuals who entered the electronic data processing profession only a few years ago. Such persons must not allow themselves to become obsolete.

The great waste is that so many organizations seem to have to learn the hard way rather than by the experience of others. So often professional data processors complain that integrity controls "cost too much." They are sadly unaware that many techniques to improve record integrity pay for themselves by also improving productivity.

A perpetual inventory system contained inaccuracies in 70% of its on-hand balances. By expanding cycle-count efforts, the rate was reduced to 30%. This then permitted a reduction of 15% in the

---

[2]*EDP Industry Report,* James Peacock, editor, International Data Corp., quoted in *Computerworld,* August 7, 1974, p. 29.

levels of inventory carried to protect against stock-outs. The reduced carrying costs saved from four times the cost of the additional controls.

Fortunately, some organizations eventually reach a state where they start to use computers creatively rather than merely extending payrolls . . . and even doing that wrong. Just as the maturation of humans is accompanied by an increasing concern for distant future events, this same phenomenon is noted in business organizations that achieve a mature level of comprehension of this invaluable tool.

A distribution company now projects anticipated future sales of each product by dividing its inventory into hundreds of demand classifications and comparing recent sales with historical sales trends for products of each type. Using this approach, they have managed to reduce inventory levels by 25% while improving the level of service.

We absolutely *must* learn to control and audit computers in a more reliable and efficient manner. Even the sophisticated applications of today barely hint at the potential of what computers will be used to do tomorrow.

One of the fundamental concepts of computers is the "stored-program" concept. This recognizes that stored programs are identical in form to stored data; therefore, programs may be modified by programs just as data can. From this recognition, we already have computer programs that appear to "learn" to play chess or to perform other advanced logic. While these applications appear to constitute "artificial intelligence," they are still merely sets of computer instructions designed by men. However, the program can modify its own instructions according to its "experience." The actual instructions that are being performed may change dynamically and be unrecognizable when compared to the original set. If we can't even design a receivables-aging program that operates correctly by using the same logic rules for years, how are we ever going to control or audit a program that changes itself each second?

What we are really witnessing is a "computer revolution" that has potentially greater consequences than the Industrial Revolution. While the Industrial Revolution harnessed machines to multiply the power of man's muscles, computers can be harnessed to multiply the power of his mind. The successful and effective use of this power demands control. The people who can provide this control will be able to guide the future.

This book was written expressly for those who are concerned about the future of their organizations and the impact computers and computer control will have upon them. For a capsule summary of what this book is and what it is not, read chapter 1.

Contents

Contents

LIST OF FIGURES AND ILLUSTRATIONS