

# EDP AUDITING

Conceptual  
Foundations  
and Practice

Ron Weber

# EDP AUDITING

---

## CONCEPTUAL FOUNDATIONS AND PRACTICE

---

**Ron Weber**

University of Queensland, Australia

**McGRAW-HILL BOOK COMPANY**

New York St. Louis San Francisco Auckland Bogotá  
Hamburg Johannesburg London Madrid Mexico Montreal New Delhi  
Panama Paris São Paulo Singapore Sydney Tokyo Toronto

# FOR MY PARENTS

This book was set in Times Roman by Ruttle, Shaw & Wetherill, Inc.  
The editors were Donald G. Mason and Edwin Hanson;  
the production supervisor was Phil Galea.  
New drawings were done by Danmark & Michaels, Inc.  
R. R. Donnelley & Sons Company was printer and binder.

## **EDP AUDITING**

### **Conceptual Foundations and Practice**

Copyright © 1982 by McGraw-Hill, Inc. All rights reserved. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher.

2 3 4 5 6 7 8 9 0 DODO 8 9 8 7 6 5 4 3 2

### **Library of Congress Cataloging in Publication Data**

Weber, Ron.

EDP auditing.

Includes index.

1. Electronic data processing departments—  
Auditing. 2. *Electronic data processing departments*  
—Auditing—Problems, exercises, etc. I. Title.  
HF5548.2.W38 657'.453 80-28872  
ISBN 0-07-068830-3

---

# PREFACE

---

A friend and colleague once said to me: "To be a good auditor you have to be better at business than your client." I've often pondered that remark, for on the one hand it is a compelling notion, yet on the other it sets an impossible ideal for auditors to achieve. Perhaps in the more traditional areas of auditing we, as auditors, are gaining confidence in the soundness of our methodologies. Admittedly, the lawsuits still prevail, but the problems seem to be in the application of the methodologies rather than in the methodologies themselves.

In the domain of modern auditing, however, we have an Achilles heel: our methodologies for the control and audit of computer systems are still in their infancy. Further, the rate at which new computer technology is developed and introduced seems to outstrip the rate at which we can develop viable audit methodologies. It is the area of EDP auditing that currently represents the great challenge to auditors.

EDP auditing is the process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, achieves organizational goals effectively, and consumes resources efficiently. Safeguarding assets involves ensuring that they are protected from damage or destruction, unauthorized use, and being stolen. Data integrity is a state: it means data is accurate, complete, and consistent. Asset safeguarding and data integrity always have been the concern of auditors. However, the definition of EDP auditing proposed also encompasses a concern for the effectiveness with which EDP systems meet their objectives and the efficiency with which data is processed. Since EDP expenditure often is a major item in an organization's balance sheet and income statement, currently management is more frequently asking auditors to evaluate these aspects of EDP systems.

## **Some Pedagogical Issues**

Before writing this book, I thought long and hard about the approach I should use to present the subject matter of EDP auditing. It seems to me there are



two approaches. With the first approach, which I will call the “exposures approach,” the writer focuses primarily on the types of losses that can occur in computer systems. The secondary focus is on the controls used to reduce these losses. With the second approach, which I will call the “controls approach,” the primary focus is on the controls and the secondary focus is on the losses that the controls reduce.

Why can't *both* exposures and controls be the primary focus? Both certainly have major importance from an audit perspective. The problem is that there is not a one-to-one relationship between exposures and controls. A single control can reduce the loss from multiple exposures. Thus, if the writer focuses on *exposures*, some subject matter on controls will be repeated; alternatively, if the writer focuses on *controls*, some subject matter on exposures will be repeated. As my students have not hesitated to point out, the writer who does not carefully control the duplication of material that results, will bore the reader quickly. The only solution, I believe, is for the writer to adopt either exposures or controls as the primary focus; the secondary focus then becomes the material that must be duplicated as efficiently as possible so presentation of the subject matter of EDP auditing is complete.

In this book, I chose to focus on *controls* for three major reasons. First, I trust that students who have had a first course in auditing will be familiar with the major types of exposures facing an organization (these do not change with computers); I assume they are reading this book because their knowledge of computer control technology is not so well developed. Second, my experience is that students feel more comfortable with the controls approach; they seem to find it less “messy” than the exposures approach. I am unsure why this is the case, but I think it has to do with controls requiring a smaller “chunk” of understanding than exposures. Third, a major purpose of this book is to integrate the burgeoning literature on computer controls that appears in *both* the auditing and computer science areas. It dismays me that each area still tends to ignore the other; each has much to contribute to the other.

The controls approach has its problems. The subject matter on computer controls is somewhat more volatile than the subject matter on exposures. Some control technology is still evolving; for example, several problems remain to be solved relating to the use of cryptography in communications networks. But I believe there to be more than enough stability in the control technology to make the approach that I have adopted worthwhile.

### Structure of the Book

The parts (and chapters) of the book follow a natural sequence. The first part motivates the EDP audit function within an organization. The second and third parts describe the computer control frameworks that should exist in an organization at the management level and application system level, respectively. By first evaluating the management control framework, the EDP auditor determines the extent and scope of testing needed at the application system level. Techniques of evidence collection are discussed in the fourth

part of the book; and the fifth part discusses how the evidence collected can be evaluated. The final part discusses the futures of EDP auditing.

One point must be made on the subject matter of the chapters. As a potential reader, you may look for chapters on the specialized areas of EDP audit: online realtime systems, database management systems, service bureaus, etc. You may be disappointed to find these chapters missing. However, through experience I am convinced that this is not the best way to initially present the subject matter of EDP auditing. Many of the controls and audit methodologies needed for online systems are the same for database management systems, and so forth. This is not to deny there are specialized controls and specialized audit techniques for these specialized areas. However, organizing the basic subject matter of EDP auditing by these specialized areas results in substantial duplication of material and frustrations for both the instructor and student. The secret of being a good EDP auditor is to be capable of assembling the fundamental controls and EDP audit methodologies in a manner appropriate for a specific computer installation, be it a simple batch system or a complex database management system.

### **Using the Book**

I intend this book to be of use primarily to both students and practitioners of EDP auditing. However, I hope it will also prove useful to EDP managers, systems analysts, and programmers who have responsibility for designing and implementing controls in systems.

The book presumes the reader has at least a basic knowledge of auditing, computer data processing, and a programming language (preferably COBOL). Thus, it is not intended for beginners in the field. The beginner should first study one of the many excellent introductory texts in the areas of auditing and computers.

At the college level, the book provides sufficient material for a solid semester's work at the upper undergraduate or graduate level. The instructor may wish to leave out some chapters—for example, Chapter 3 on organization and management of the EDP audit function—and give more emphasis to others. The chapter bibliographies are a source of additional reading for students if the instructor wants to spend more time on particular chapters.

Besides the usual lecture method, the instructor might like to try using the book employing a case study approach. The students are made responsible for studying the chapter materials; the class periods are used to discuss the exercises and cases at the end of each chapter.

Besides the exercises and cases, each chapter in the book also contains a set of review questions. In general, answers to the review questions can be found in the chapter. At times, however, a little thought may be required. The exercises and cases are more demanding. Often I have tried to make the student think from an exposures perspective, thereby compensating for my primary focus on controls in the chapter. The exercises and cases also may require the student to integrate material covered in earlier chapters. To assist

the instructor, there is also an instructor's manual available containing suggested solutions to the assignment material.

I strongly recommend that the instructor supplement the assignment material with further case studies and some computer problems. The case studies should be more comprehensive than the short cases contained in the book so the student is forced to integrate the text material. They might be on specific types of systems; for example, an online banking system or a service bureau. A variety of computer problems can be set; for example, using a generalized audit software package to examine the quality of data on a file or using a test data generator to assist validating the logic of a program.

I hope that as a user of the book, you conclude that the benefits exceed the costs. I would appreciate your feedback, whether it be positive or negative, so that a second edition (if it occurs) might better meet your needs.

## ACKNOWLEDGMENTS

This book grew from a set of notes prepared for a course on EDP Auditing that I taught with Professor Gordon B. Davis during my graduate student days at the University of Minnesota from 1973–1976. The opportunity to teach the course is simply one of many opportunities for professional and intellectual development that Professor Davis has given me during my association with him. I cannot express properly my deep appreciation to him for his ongoing support and encouragement.

I owe, also, a large intellectual debt to Professor Gordon C. Everest at the University of Minnesota. His research on database management systems and his clear thinking on data integrity have significantly influenced my own thinking.

I was privileged to have five reviewers of the manuscript who, in spite of my limitations as a writer, were always tremendously supportive of my efforts. Professors Gordon B. Davis, University of Minnesota; Russell C. Kick, Jr., University of North Florida; John O. Mason, Jr., University of Alabama; Frederick L. Neumann, University of Illinois; and Carl S. Warren, University of Georgia, all reviewed portions or the whole of the manuscript. Their suggestions improved considerably its overall quality.

The typing of the manuscript was handled expertly, efficiently, and cheerfully by five women. Chris Stone and Liz Kinloch prepared some of the initial chapters while I was at the Australian National University in Canberra. Lynn Gallegos and Sage Toninato typed chapter revisions while I was on leave at the University of Minnesota. The bulk of the work, however, has been done by Jo Waldron at the University of Queensland.

Finally, to the two women in my life—my wife, Kay, and my daughter, Amy—go my deepest thanks. The debt I owe them for their love, support, and patience is awesome.

*Ron Weber*

---

# CONTENTS

---

|               |   |           |
|---------------|---|-----------|
|               | PREFACE   | xi        |
| <b>PART 1</b> | <b>INTRODUCTION</b>   |           |
| <b>1</b>      | <b>OVERVIEW OF EDP AUDITING</b>                                     | <b>3</b>  |
|               | Need for Control and Audit of Computers                             | 4         |
|               | EDP Auditing Defined  | 7         |
|               | Effects of EDP on Internal Control                                  | 10        |
|               | Foundations of EDP Auditing   | 12        |
| <b>2</b>      | <b>A GENERAL APPROACH TO EDP AUDITING</b>                           | <b>21</b> |
|               | The System of Internal Controls and the Audit Approach              | 22        |
|               | Controls and the Potential for Loss                                 | 22        |
|               | The Nature of Computer Controls                                     | 24        |
|               | Overview of Steps in an EDP Audit                                   | 28        |
|               | Some Major Audit Decisions  | 32        |
| <b>3</b>      | <b>ORGANIZATION AND MANAGEMENT OF THE EDP<br/>AUDIT FUNCTION</b>    | <b>45</b> |
|               | Need for a Separate EDP Audit Section                               | 46        |
|               | Centralization versus Decentralization of the EDP<br>Audit Function | 50        |
|               | Staffing the EDP Audit Function                                     | 51        |
|               | Training  | 53        |
|               | Relationships with Management and Other<br>Organization Groups      | 57        |



|   |    |
|---|----|
| Promotional Opportunities for the EDP Auditor | 59 |
| Life Cycle of the EDP Audit Group             | 60 |

## **PART 2 THE MANAGEMENT CONTROL FRAMEWORK**

|          |   |            |
|----------|---|------------|
| <b>4</b> | <b>TOP MANAGEMENT AND EDP MANAGEMENT</b>                      | <b>69</b>  |
|          | Evaluating the Planning Function                              | 70         |
|          | Evaluating the Organizing Function                            | 78         |
|          | Evaluating the Staffing Function                              | 84         |
|          | Evaluating the Directing Function                             | 86         |
|          | Evaluating the Controlling Function                           | 88         |
| <b>5</b> | <b>SYSTEMS DEVELOPMENT</b>                                    | <b>98</b>  |
|          | Auditing the System Development Process                       | 99         |
|          | Normative Models of the System Development Process            | 99         |
|          | Evaluating the Major Phases in the System Development Process | 103        |
| <b>6</b> | <b>PROGRAMMING MANAGEMENT</b>                                 | <b>128</b> |
|          | The Program Life Cycle  | 129        |
|          | Organizing the Programming Team                               | 144        |
|          | Managing the System Programming Group                         | 148        |
|          | Software Development Aids                                     | 150        |
| <b>7</b> | <b>DATABASE ADMINISTRATION</b>                                | <b>164</b> |
|          | Motivations toward a Database Administration Role             | 165        |
|          | Some Audit Considerations                                     | 166        |
|          | Functions of the Database Administrator                       | 167        |
|          | Organizational Considerations                                 | 171        |
|          | Data Dictionary   | 172        |
|          | Control over the Database Administrator                       | 175        |
| <b>8</b> | <b>OPERATIONS MANAGEMENT</b>                                  | <b>183</b> |
|          | Overview of Operations Management                             | 184        |
|          | Computer Operations   | 185        |
|          | Data Preparation  | 189        |
|          | Control Section   | 190        |
|          | File Library  | 191        |
|          | Documentation Library   | 194        |
|          | Security Section  | 195        |

**PART 3 THE APPLICATION CONTROL FRAMEWORK**

|           |  |            |
|-----------|--|------------|
| <b>9</b>  | <b>DATA CAPTURE, PREPARATION, AND ENTRY CONTROLS</b> | <b>209</b> |
|           | Overview of Data Capture, Preparation, and Entry     | 211        |
|           | Evaluation of Data Capture Methods                   | 212        |
|           | Evaluation of Data Preparation/Entry Methods         | 216        |
|           | Source Document Design                               | 224        |
|           | Interactive Language Design                          | 227        |
|           | Data Code Controls                                   | 231        |
|           | Check Digits   | 234        |
|           | Batch Controls                                       | 237        |
|           | Other Data Capture and Preparation Controls          | 239        |
| <b>10</b> | <b>ACCESS AND COMMUNICATIONS CONTROLS</b>            | <b>249</b> |
|           | Access Controls                                      | 250        |
|           | Communications Controls                              | 260        |
|           | Cryptography   | 270        |
| <b>11</b> | <b>INPUT CONTROLS</b>                                | <b>283</b> |
|           | Input Validation Checks                              | 285        |
|           | Design of the Input Program                          | 288        |
|           | Control over Input                                   | 294        |
|           | A Generalized Input System                           | 295        |
| <b>12</b> | <b>PROCESSING CONTROLS</b>                           | <b>304</b> |
|           | Validation Checks                                    | 305        |
|           | Some Matters of Programming Style                    | 306        |
|           | Concurrency Control                                  | 311        |
|           | System Software Integrity                            | 316        |
|           | Control over Hardware Malfunctions                   | 321        |
|           | Checkpoint/Restart Controls                          | 323        |
| <b>13</b> | <b>OUTPUT CONTROLS</b>                               | <b>330</b> |
|           | Controls over Reports                                | 331        |
|           | Interrogation Languages and Output Response Errors   | 340        |
|           | Controls over Files                                  | 343        |
|           | Some Output Effectiveness/Efficiency Considerations  | 343        |
| <b>14</b> | <b>AUDIT TRAIL CONTROLS</b>                          | <b>355</b> |
|           | The Accounting Audit Trail                           | 356        |
|           | The Operations Audit Trail                           | 366        |

|               |   |            |
|---------------|---|------------|
| <b>15</b>     | <b>BACKUP AND RECOVERY CONTROLS</b>                         | <b>376</b> |
|               | Need for Backup and Recovery                                | 377        |
|               | Backup and Recovery Strategies                              | 378        |
|               | Some Administrative Aspects                                 | 393        |
| <b>PART 4</b> | <b>EVIDENCE COLLECTION</b>                                  |            |
| <b>16</b>     | <b>GENERALIZED AUDIT SOFTWARE</b>                           | <b>401</b> |
|               | Motivations for Generalized Audit Software Development      | 402        |
|               | Functional Capabilities                                     | 403        |
|               | Audit Tasks That Can Be Accomplished                        | 406        |
|               | Functional Limitations                                      | 409        |
|               | Installation/Audit Group Maturity Issues                    | 410        |
|               | Managing a Generalized Audit Software Application           | 412        |
|               | Accessing Complex Data Structures                           | 414        |
|               | Purchasing Audit Software                                   | 419        |
| <b>17</b>     | <b>SYSTEM SOFTWARE AND SPECIALIZED AUDIT SOFTWARE</b>       | <b>431</b> |
|               | System Software as an Audit Tool                            | 432        |
|               | Specialized Audit Software as an Audit Tool                 | 440        |
| <b>18</b>     | <b>CODE REVIEW, TEST DATA, AND CODE COMPARISON</b>          | <b>448</b> |
|               | Factors That Lower Program Quality: Some Empirical Evidence | 450        |
|               | Program Source Code Review                                  | 451        |
|               | Test Data   | 458        |
|               | Program Code Comparison                                     | 465        |
| <b>19</b>     | <b>CONCURRENT AUDITING TECHNIQUES</b>                       | <b>473</b> |
|               | Basic Nature of Concurrent Auditing Techniques              | 474        |
|               | Need for Concurrent Auditing Techniques                     | 474        |
|               | Types of Concurrent Auditing Techniques                     | 477        |
|               | Implementing Concurrent Auditing Techniques                 | 485        |
|               | Advantages/Disadvantages of Concurrent Auditing Techniques  | 487        |
| <b>20</b>     | <b>INTERVIEWS, QUESTIONNAIRES, AND CONTROL FLOWCHARTS</b>   | <b>493</b> |
|               | Interviews  | 494        |
|               | Questionnaires  | 498        |
|               | Control Flowcharts  | 506        |

|                   |   |                |
|-------------------|---|----------------|
| <b>21</b>         | <b>PERFORMANCE MONITORING TOOLS</b>                                 | <b>515</b>     |
|                   | The Objects of Measurement  | 516            |
|                   | General Characteristics of Performance Monitors                     | 517            |
|                   | Types of Performance Monitors                                       | 518            |
|                   | Performance Monitoring and Data Integrity                           | 526            |
| <br><b>PART 5</b> | <br><b>EVIDENCE EVALUATION</b>                                      |                |
| <b>22</b>         | <b>EVALUATING ASSET SAFEGUARDING AND DATA INTEGRITY</b>             | <b>535</b>     |
|                   | Measures of Asset Safeguarding and Data Integrity                   | 536            |
|                   | Evaluating Asset Safeguarding and Data Integrity: Formal Techniques | 538            |
|                   | Cost-Effectiveness Considerations                                   | 545            |
|                   | Some Informal Guidelines for Evaluation                             | 553            |
| <b>23</b>         | <b>EVALUATING SYSTEM EFFECTIVENESS</b>                              | <b>560</b>     |
|                   | Goals of an Information System                                      | 561            |
|                   | The Evaluation Process  | 562            |
|                   | The Global Evaluation Judgment                                      | 576            |
| <b>24</b>         | <b>EVALUATING SYSTEM EFFICIENCY</b>                                 | <b>583</b>     |
|                   | The Evaluation Process  | 584            |
|                   | Performance Indices   | 587            |
|                   | Workload Models   | 588            |
|                   | System Models   | 593            |
| <br><b>PART 6</b> | <br><b>FUTURES</b>  |                |
| <b>25</b>         | <b>THE CHANGING EDP AUDIT FUNCTION</b>                              | <b>609</b>     |
|                   | Toward Professionalism  | 610            |
|                   | Legal Influences  | 612            |
|                   | Social Influences   | 616            |
|                   | Impact of the Changing Technology                                   | 619            |
|                   | Research and Pedagogy   | 624            |
|                   | <br><b>INDEXES</b>  | <br><b>629</b> |
|                   | Name Index  |                |
|                   | Subject Index   |                |

# PART ONE

## INTRODUCTION

EDP auditing is a function that has been developed to assess whether computer systems safeguard assets, maintain data integrity, and achieve the goals of an organization effectively and efficiently. Parties both internal and external to an organization are concerned with whether computer systems fulfill these objectives. The management of an organization attempts to use resources in an optimal manner within the constraints established by the society; for example, management may pursue a profit-maximizing objective subject to the

| Chapter   | Overview of contents  |
|---|---|
| 1 Overview of EDP Auditing                              | Discusses the need for control and audit of computers; defines EDP auditing; examines the underlying support disciplines; evaluates the effects of EDP on internal control  |
| 2 A General Approach to EDP Auditing                    | Examines the effects of the system of internal controls on the audit approach; discusses the <i>relationship between expected losses and errors</i> and irregularities; discusses the nature of computer controls; provides an overview of the steps in an EDP audit; describes some of the major EDP audit decisions |
| 3 Organization and Management of the EDP Audit Function | Discusses setting up and organizing an EDP audit group; considers staffing and training issues; examines the relationship of the EDP audit group with other organizational groups   |

legal constraint that it maintains the privacy of data provided to it by individual members of the society. External parties, whether they be shareholders, unions, or pressure groups, also have vested interests in how organizations use computers. Their concerns vary from wealth maximization to possible work displacement to a loss of personal privacy.

The first three chapters of this book introduce the EDP audit function. They discuss the motivations for an EDP audit function, the objectives of EDP auditing, present an overview of the EDP audit process, and show how the EDP audit function might be set up within an organization.



---

# **OVERVIEW OF EDP AUDITING**

---

## **CHAPTER OUTLINE**

### **NEED FOR CONTROL AND AUDIT OF COMPUTERS**

- Organizational Costs of Data Loss
- Incorrect Decision Making
- Computer Abuse
- Privacy
- Controlled Evolution of Computer Use

### **EDP AUDITING DEFINED**

- Asset Safeguarding Objectives
- Data Integrity Objectives
- System Effectiveness Objectives
- System Efficiency Objectives

### **EFFECTS OF EDP ON INTERNAL CONTROL**

- Separation of Duties
- Access to Assets
- Types of Internal Controls
- The Audit/Management Trail
- Comparing Recorded Accountability with Assets
- Consequences of Error

### **FOUNDATIONS OF EDP AUDITING**

- Traditional Auditing
- Information Systems Management
- Behavioral Science
- Computer Science

**SUMMARY**

**REVIEW QUESTIONS**

**EXERCISES AND CASES**

**REFERENCES**

Whereas 25 years ago we fulfilled most of our data processing needs manually, today computers perform much of the data processing required in both the private and public sectors of our economy. The need to maintain the integrity of data processed by computers pervades our lives. We have increasing fears that our substantially increased data processing capabilities are not well controlled. The media makes much of computer abuse. We have concerns about the privacy of data we exchange with organizations such as the tax department, medical authorities, and credit granting institutions. Probably all of us have suffered the frustrations of trying to get an organization to update its computer-maintained name and address file.

Uncontrolled use of computers has a widespread impact on a society. Inaccurate information causes misallocation of resources within the economy. Frauds are perpetrated because of inadequate system controls. Unfortunately, the person who suffers most is often the person who can least afford to suffer; for example, the small shareholder and the low-income earner. Perhaps more subtle is the growing distrust of institutions that gather and process large volumes of data. A sense of lost individuality now exists: the “big brother” of 1984 is upon us.

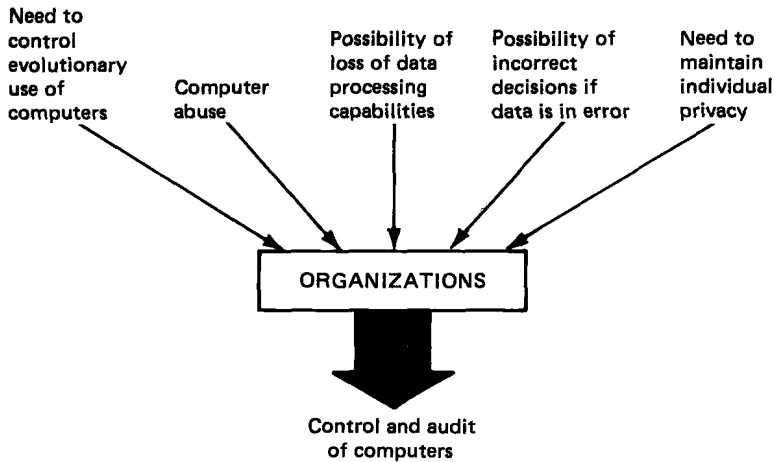
**NEED FOR CONTROL AND AUDIT OF COMPUTERS**

Computers continue to be used more extensively to process data. Between 1974 and 1979, International Data Corporation [1979] estimated worldwide use of U.S. manufactured computers increased from 264,690 units to 764,400 units. As part of this increase, worldwide use of U.S. manufactured minicomputers grew from an estimated 135,300 units in 1974 to an estimated 504,700 units in 1979. Steady growth in computer use, especially minicomputer use, is inevitable.

Since computers play such a large part in assisting us process data, it is important that their use be controlled. The following sections briefly discuss five major reasons for setting up a function to examine controls over computer data processing (Figure 1.1).

**Organizational Costs of Data Loss**

Data is a critical resource necessary for an organization’s continuing operations. Everest [1982] proposes that data provides the organization with an



**Figure 1.1**  
Factors influencing an organization toward control and audit of computers.

image of itself, its environment, its history, and its future. If this image is accurate, the organization increases its abilities to adapt and survive in a changing environment.

Consider the case of a large department store that has its accounts receivable file destroyed. Unless its customers are honest, and also remember what they have purchased from the store, the firm can suffer a major loss in cash receipts and its long-run survival may be affected. Consider, also, the department store losing its accounts payable file. It is unable to pay its accounts on time and can suffer a loss of credit rating as well as any discounts available for early payment. If it contacts creditors requesting assistance, the department store relies on the honesty of the creditors in notifying it of the amounts owed. Further, creditors must now question the competence of the department store's management and may be unwilling to extend credit in the future.

Such losses can arise through lax controls existing over computers. Management may not provide adequate backup for computer files; thus, the loss of a file through computer program error, sabotage, or natural disaster means the file cannot be recovered and the organization's continuing operations are impaired.

### **Incorrect Decision Making**

The importance of accurate data depends on the types of decisions made by individuals having some interest in an organization. For example, if management makes strategic planning decisions, most likely they will tolerate some