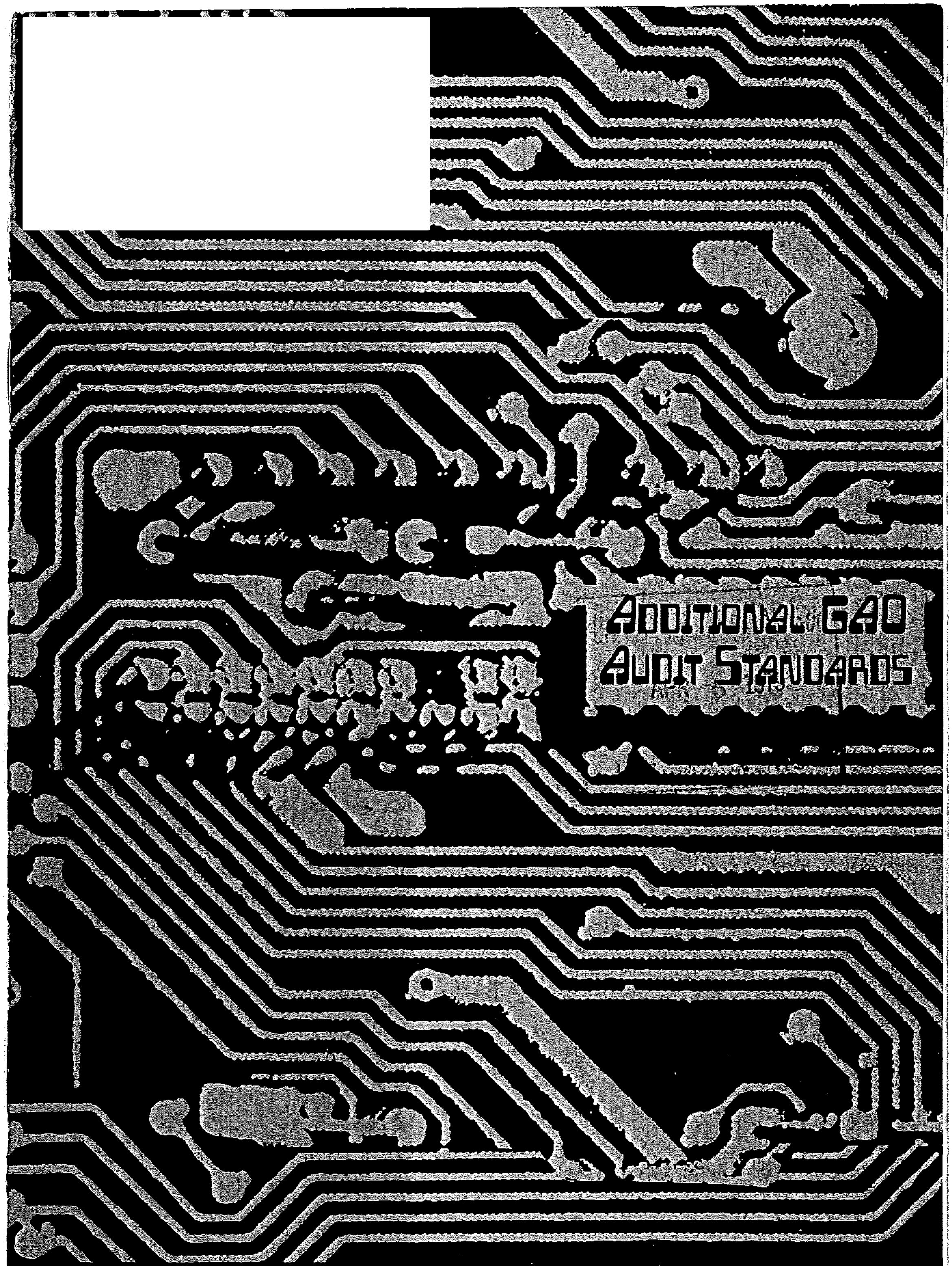


ADDITIONAL GAO AUDIT STANDARDS

AUDITING COMPUTER-BASED SYSTEMS

Foreword

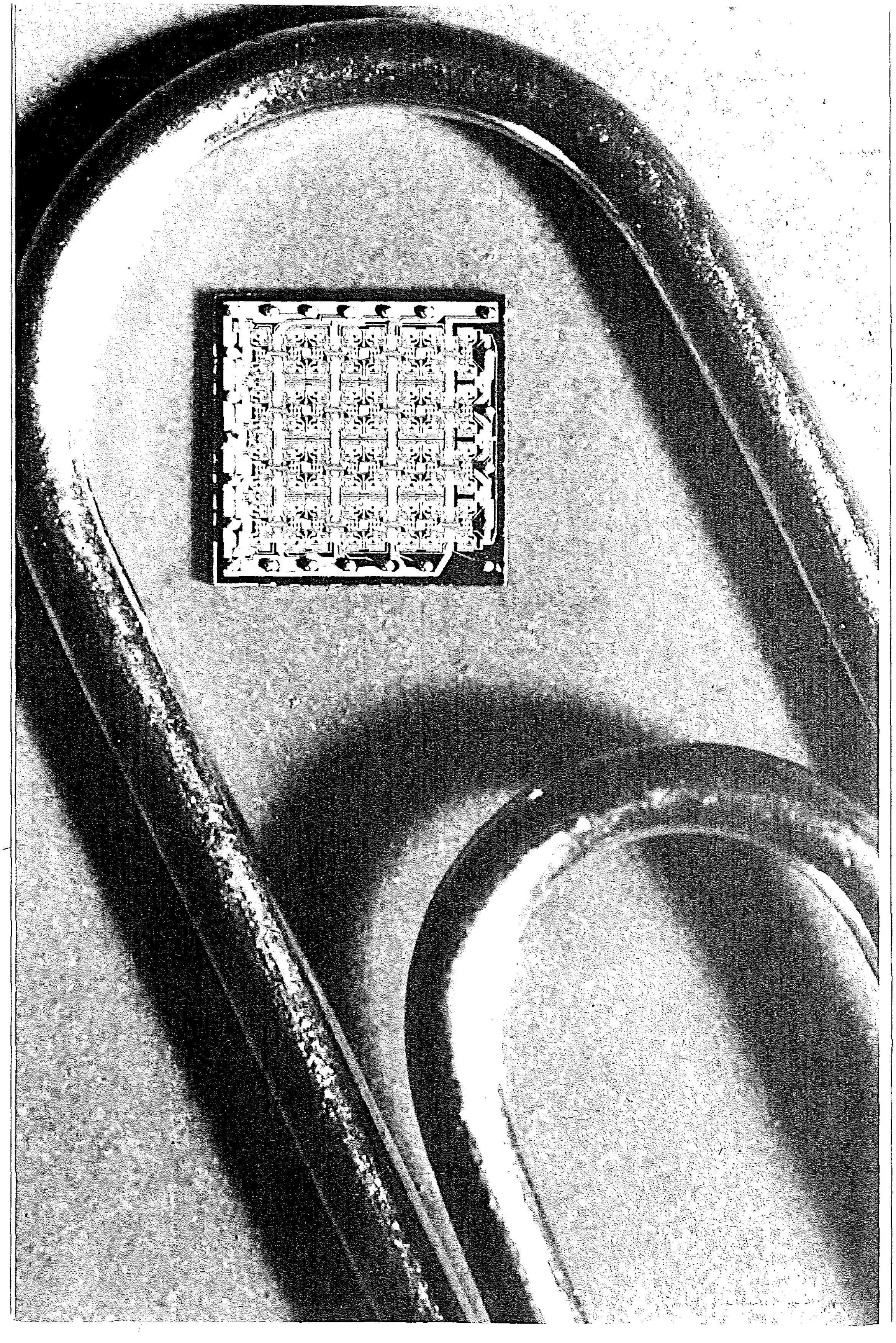
Our office has been concerned for some time that the audit coverage accorded computer-based systems does not measure up to the quality needed to assure that proper results are attained. Our study of the area has led to the development of supplemental audit standards to provide guidance for auditors involved in such work.

As noted in the Introduction, these standards are effective January 1, 1980, and earlier compliance is encouraged. They will be incorporated in the next revision of the basic document "Standards for Audit of Governmental Organizations, Programs, Activities & Functions."

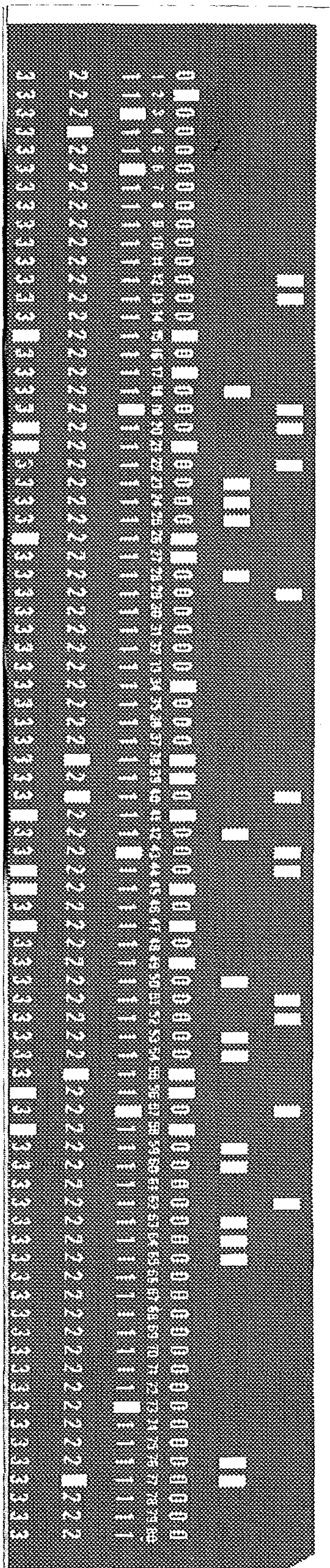
Elmer B. Staats
Comptroller General
of the United States
March, 1979

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402

Stock Number 020-000-00174-7



Contents



Introduction

In 1972, GAO issued the pamphlet "Standards for Audit of Governmental Organizations, Programs, Activities & Functions," (the "Yellow Book"). This publication discussed the role of the auditor resulting from an increasing demand for information in a far more complex society that expects more services from governmental units at all levels. Adding complexity to providing such information in an economic, efficient, and effective manner has been the emergence of the electronic digital computer.

With the computer becoming more complex through the development of sophisticated multiprograming capacity, coupled with telecommunication links and a wide variety of new input and output devices, another dimension has been added to the role expected of the auditor. In order for him to fulfill his professional responsibilities, the auditor must now be able to perform a wide variety of tasks which, until recently, did not exist or were not considered within the auditor's scope.

For example, when manual systems were audited, a wide variety of approaches were generally available and the most appropriate would be selected for the given circumstances. If there were control weaknesses, corrective changes were easily formulated and suggested. However, it is now possible to produce a data processing system with such poor controls that neither the auditor nor the manager can place reliance on the system's integrity. For this reason, audit review during the design and development process of an automated system has become crucial if management is to be provided needed assurance that auditable and properly controlled systems are being produced.

Moreover, once systems are placed in operation, the auditor has a continuing requirement to review both general controls and application controls. Such reviews are to assure that systems support management policy and produce reliable results. For a system already in operation when an audit is scheduled, the auditor should determine whether the system's objectives are being met.

This publication is supplemental to the basic standards set forth in the "Yellow Book." This material will be incorporated in the next revision of the document.

These supplemental standards are consistent with the concepts of the "1978 Report, Conclusions, and Recommendations of the AICPA's Commission on Auditors Responsibilities," which states that:

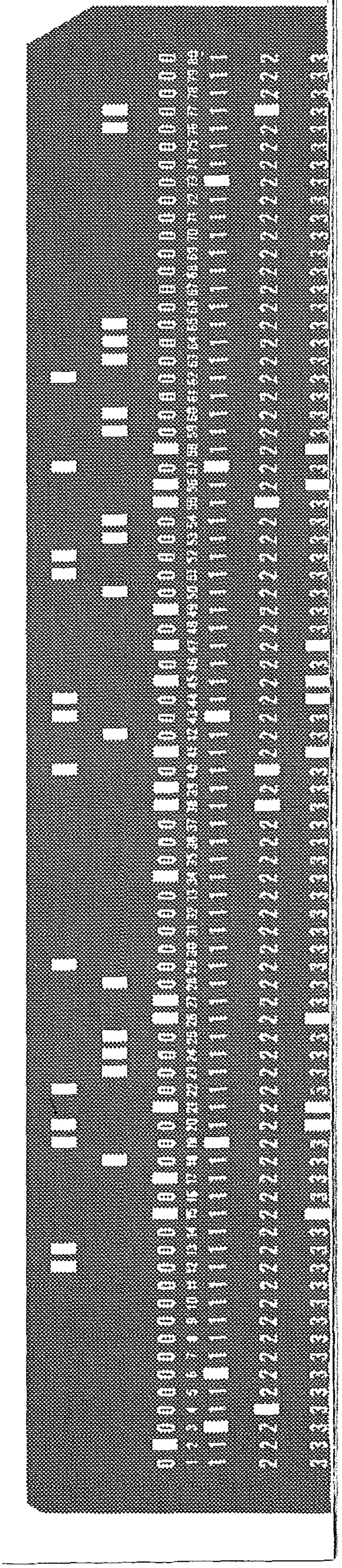
> "The auditor's study and evaluation of the internal accounting control system should be expanded beyond what is now required by generally accepted auditing standards. The auditor should review and test the entire accounting control system. The objective of this study and evaluation would be to enable the auditor to reach a conclusion on whether controls over each significant part of the accounting system provide reasonable, though not absolute, assurance that the system is free of material weaknesses."

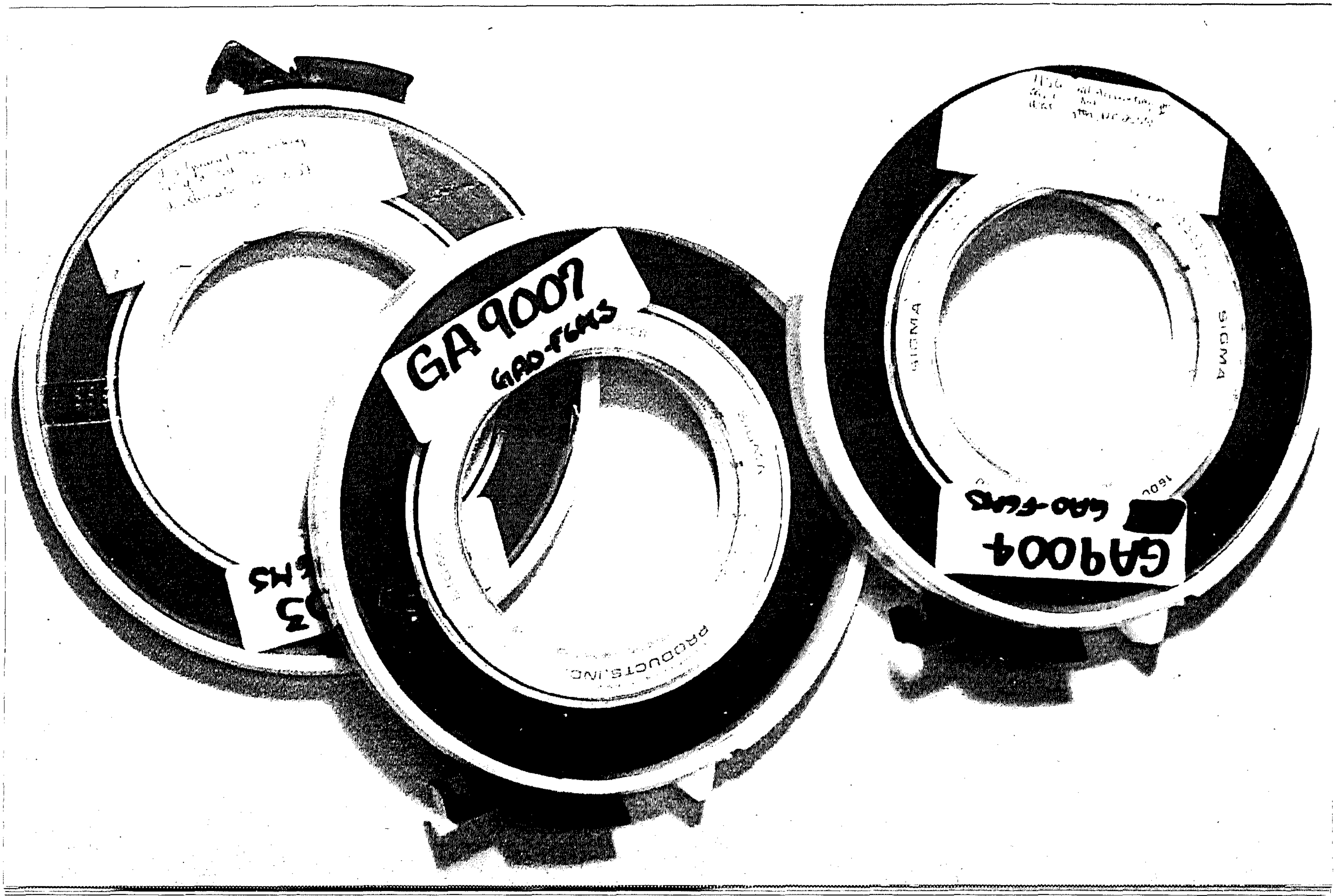
and that

> "The standard of professional skill and care should be amplified to require a study and evaluation of controls that have a significant bearing on the presentation and detection of fraud."

* * *

These supplemental standards are effective January 1, 1980, although earlier compliance is encouraged.




GA9007
GAO-FLAGS
PRODUCTS, INC.
SIGMA
GA9004
[redacted] GAO-FLAGS
SIGMA
SIGMA
1600
3
MS

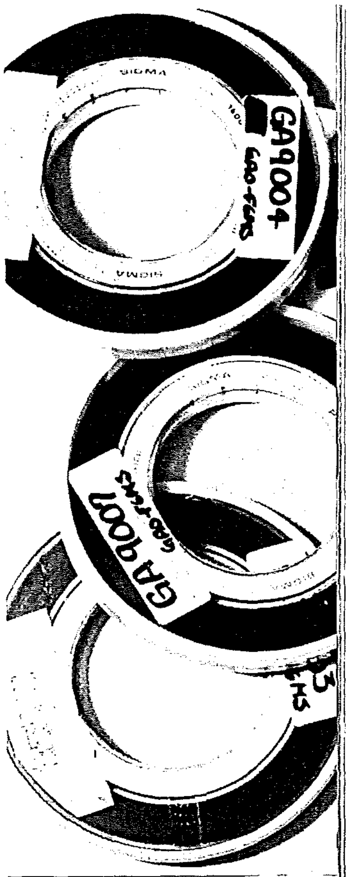
Summary of Supplemental Standards

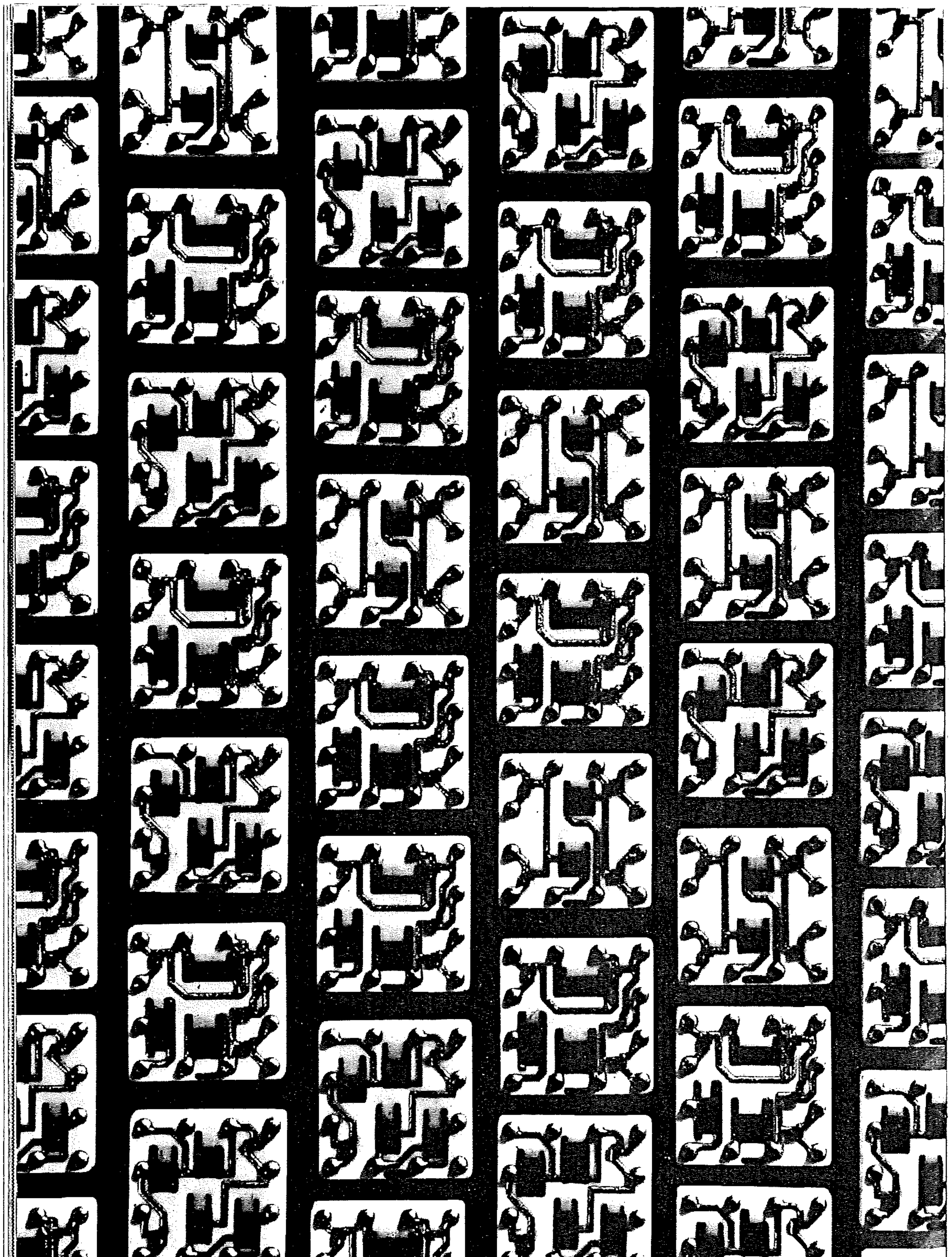
The work of the auditor has expanded significantly with the evolution of the computer. To maintain professionalism in the performance of audit work three supplemental standards apply, as listed below.

Supplemental Standards

1. The auditor shall actively participate in reviewing the design and development of new data processing systems or applications, and significant modification thereto, as a normal part of the audit function.
2. The auditor shall review general controls in data processing systems to determine that (A) controls have been designed according to management direction and legal requirements, and (B) such controls are operating effectively to provide reliability of, and security over, the data being processed.
3. The auditor shall review application controls of installed data processing applications to assess their reliability in processing data in a timely, accurate, and complete manner.

These three supplemental standards are presented and discussed in the succeeding sections.





Supplemental Standard for Internal Audit Role During System Design and Development

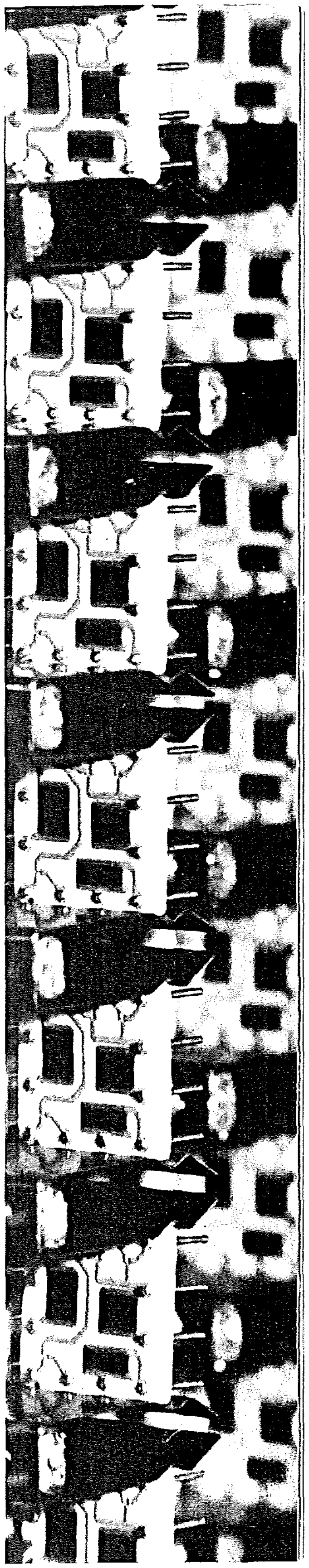
The first supplemental standard for computer-related auditing is

> "The auditor shall actively participate in reviewing the design and development of new data processing systems[1] or applications, and significant modifications thereto, as a normal part of the audit function."

GAO recognizes that compliance with this standard may not always be feasible. Internal auditors may require additional specific managerial authorization or direction to perform this work and external auditors may need a special engagement. However, compliance with this standard should always be an auditing goal.

Whenever management approval to perform such work has not already been given, the auditor has a duty to alert management of the potential results of such restriction. The auditor should formally communicate to management information on the possible adverse effects of not requiring audit review and evaluation of automated systems design and development processes. Such communication should point out that, in the absence of effective audit of the system design and development processes, the resultant systems

- may not possess the built-in controls necessary to assure proper and efficient operations,
- may not provide the capability to track events through the system and thus impede — if not completely frustrate — audit review of the system in operation, and,
- (for financial systems) may not comply with generally accepted accounting principles and, may result in qualifications of the accountant's opinion on the financial statements.



[1] Includes software matters, as well as hardware configuration decisions.

GAO believes that once management has been properly alerted, the auditor will be directed to comply with this standard. Management's denial of the authority to comply with the standard, after receiving the auditor's message, will relieve the auditor of responsibility for work in this area.

Underlying rationale

Both auditors and management officials have interest in assuring that system design, development, and overall operations achieve the objectives of adequate internal controls and effective auditability.[2] For systems already in existence when audits are made, the auditor should determine whether the objectives of the systems are being achieved.

As capabilities of computer-based information systems have grown, the systems and applications have grown more complex and interrelated. Initially, there were separate automated applications for personnel, payroll, and labor cost accounting. Each application or system would be processed independently of the other, and their input material would be generated from separate and distinct sources, and be processed against separate data files.

With the integration of application systems now being encountered, the payroll, personnel, and labor-cost-accounting applications can be interrelated subsystems of a far larger online system, and the outputs of one subsystem can now be the inputs for another without any human review. Thus, a control weakness in one segment of the system may have completely unanticipated effects in other segments with a cascading of unanticipated effects causing catastrophic results. Such mistakes, waste, and general confusion may even adversely affect the organization's viability.

The objectives of requiring auditor participation in system design, development, and modification are set forth below, with comments on each.

Management Policies

Objective 1: To assure that systems/applications faithfully carry out the policies management has prescribed for the system.

Policies setting forth what is expected of ADP systems should be established by management, and the auditor should determine whether

[2] Because of the uniqueness of the contract audit environment, it is unlikely that the contract auditor will be able to comply fully with this standard. However, the contract auditor may partially accomplish the objectives of the standard by determining the extent and effectiveness of the work of the company's internal auditors or outside accountants in the design and development phase.

these policies are being carried out in the design. The auditor should ascertain that an appropriate approval process is being followed, both in the development of new systems and in the making of modifications to existing systems. The auditor should consider the need for approval of the system's design by data processing management, user groups, and other groups whose data and reports may be affected. Also, the auditor should review the provisions for security that are required by management to protect data for programs against unauthorized access and modification.

If management's requirements are not being met, the auditor has the responsibility to report such shortcomings to the appropriate officials who can effect corrective action. Frequently in the past, efforts to bring new systems/applications on the air by scheduled dates have resulted in some management-desired elements or controls being set aside by system designers, for later consideration. The auditor, in retaining his independence during the system design and development cycle, should report such actions to top management for appropriate resolution.

Audit Trail

Objective 2: To provide assurance that systems/applications provide the controls and audit trails needed for management, auditor, and operational review.

In financial applications, it is considered a basic tenet that there be a capability to trace a transaction from its initiation, through all the intermediate processing steps, to the resulting financial statements. Similarly, information in the financial statements must be traceable to its origination. Such capability is referred to by a variety of terms—audit trail, management trail, transaction trail, etc. — and is also highly essential in nonfinancial systems/applications. A proper assessment of the reliability of the output can be made only when each step can be isolated and the controls over it (both manual and automated) can be evaluated.

Audit review of the system design and development process can help assure management that this capability is in fact being engineered into the system/application.

Controls

Objective 3: To provide assurance to management that systems/applications include the controls necessary to protect against loss or serious error.

The system design and development processes include (1) definition of the processing to be carried out by a computer, (2) design of the processing steps to the followed, (3) determination of the data input and files that will be required, and (4) specification of each individual program's input data and output. Each of these areas must be properly controlled, in consonance with good management practices, and the auditor's review of these matters must provide management assurance that the system/application, once placed in operation, will meet this objective.

(It is possible for properly designed systems, with excellent control mechanisms built in, to have these controls bypassed or overridden. This area is addressed under supplemental standards 2 and 3.)

Note that almost every system has manual aspects (e.g., input origination, output disposition) and these should be covered for adequacy by the auditor reviewing systems controls.

Efficiency and Economy

Objective 4: To provide assurance that systems/applications will be efficient and economical in operation.

Determining whether an organization is managing and utilizing its resources (personnel, property, space, etc.) in an efficient and economical manner, and reporting on the causes of inefficiencies or uneconomical practices, including inadequacies in management information systems, administrative procedures, or organizational structures, are set forth in the basic standards booklet as a basic characteristic of audit work in reviewing Government programs. With the development of complex systems/applications, the internal auditor's review should also demonstrate that operations will produce desired results at minimum cost. For example, early in the system's development stage, the auditor should review the adequacy of the (1) statement of mission needs and system objectives, (2) feasibility study and evaluation of alternative designs to meet those needs and objectives, and (3) cost-benefit analysis which attributes specific benefits and costs to system alternatives.

Legal Requirements

Objective 5: To assure that systems/applications conform with applicable legal requirements.

Legal requirements applicable to systems/applications may originate from a variety of sources. One such requirement is compliance with privacy statutes enacted at State and Federal levels, in which certain types of information about individuals are restricted as to collection and use. Appropriate safeguards are obviously necessary in such systems. Conversely, those organizations subject to the Freedom of Information Act should have systems/applications designed so that appropriate and timely response can be made to legitimate requests under the statute.

The applicability of the Federal Information Processing Standards program to the system involved should also be checked by the auditor. If such standards apply, they should be included in the auditors' review.

Once again, auditor participation in the design and development process will serve to assure management that these requirement have been considered and satisfied.

Documentation

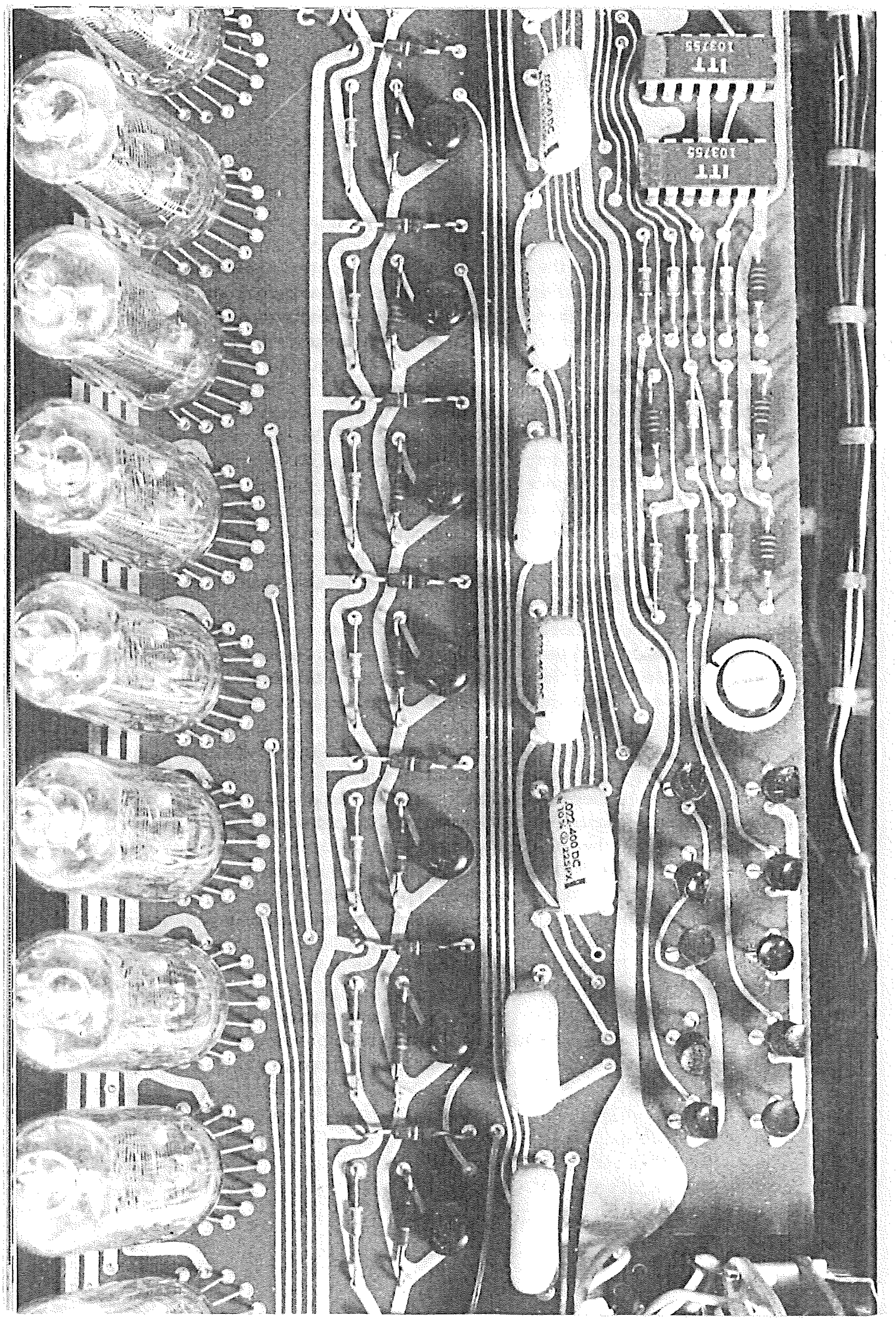
Objective 6: To provide assurance that systems/applications are documented in a manner that will provide the understanding of the system required for appropriate maintainance and auditing.

The auditor should determine whether the design/modification process produces documentation sufficient to define (1) the processing that must be performed by programs in the system, (2) the data files to be processed, (3) the reports to be prepared for users, (4) the operating instructions for use by computer operators, and (5) the user group instructions for preparation and control of data. The auditor should also ascertain whether management policy provides for evaluation of documentation and adequate test of the system before it is made operational. These steps are to assure that reliance can be placed in the system and its controls.

The methods of achieving these objectives will be determined by the circumstances attending the specific situation. Generally, such audit work will cover reviewing adequacy of management policies, examining approvals, documentation, test results, and cost studies and other data to determine whether management policies and legal requirements are being followed; and determining whether the system possesses the necessary control features and trails.

The auditor should not become part of the system design/development team to perform work under this supplemental standard. His involvement should be limited to reviewing what is being done by the team and reporting to management his objective evaluation of the effort.

At the completion of the design and development phases, and during final system testing phases, the auditor should verify that the implemented system conforms with these six objectives.


ITT
103755
ITT
103755
.022 400 DC

Standard for Audit Review of General Controls in Computer-Based Systems

The second supplemental standard is:

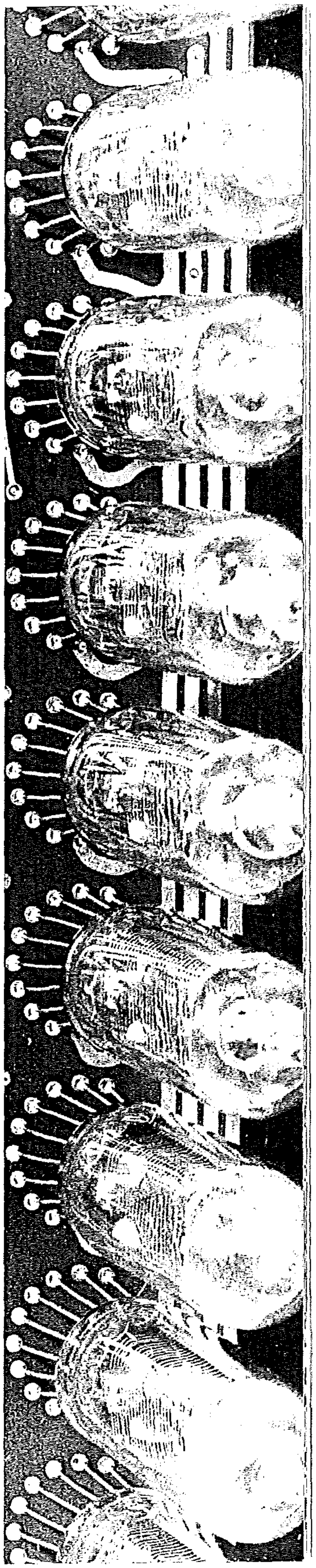
> "The auditor shall review general controls in data processing systems to determine that (A) controls have been designed according to management direction and legal requirements, and (B)suchcontrols are operating effectively to provide reliability of, and security over, the data being processed."

The transition from mechanical data processing to automatic data processing occasions the need for revision to traditional audit approaches. The complexity and far-reaching scope of such systems requires that the internal auditor give greater attention both to the system which processes data as well as to the data itself. The theory is that if the system is secure and controlled, the auditor will be able to rely on the data processed and reported.

The auditor should distinguish between general and application controls. General controls are normally applicable to all processing being carried out within the installation while application controls may vary among applications and are therefore reviewed on an individual application basis. (See supplemental standard 3 for applications control audit review.) Auditors are to review and evaluate these general controls and consider their effectiveness in performing the review of individual application controls.

Organizational Controls

Authority and responsibility must be delegated in such a manner that the organizational objectives can be met with efficiency and effectiveness. The auditor should review the organization, delegation of authority, responsibilities, and separation of duties in the organization. Such reviews are to determine whether functional lines of authority are designed to meet the organization's objectives and whether the separation of duties provides for a relatively strong level of internal control. For example, separation of duties should provide for separation among program and systems development functions, computer operations, control



over input of data, and the control group responsible for maintaining application controls. In reviewing these matters, the "total system" must be considered by the auditor.

With regard to reviewing the separation of duties, the auditor should evaluate the control strengths and report on weaknesses resulting from inadequate separation. Periodic rotation of employees and mandatory vacations may enhance management's ability to maintain adequate separation of duties. The auditor should review whether such a policy is being followed.

Physical Facilities, Personnel, and Security Controls

Adequate physical facilities and other resources (such as adequately trained personnel, supplies, and power) are necessary for the organization to meet its data processing objectives. The auditor should review these factors to determine whether or not the organization has adequate resources for meeting its needs.

Personnel management—including supervision, motivation, and professional development of personnel—is integral to the successful management of the data processing function. The auditor should review and evaluate these management policies and practices to ascertain whether the necessary policies exist and determine whether they are properly followed. For example, since the entire field of computers is rapidly evolving, the organization's personnel management office needs to development — in conjunction with the data processing organization — an education and training program. This program should keep employees abreast of current developments so that they may perform their duties most efficiently and economically, and be able to use new methods whenever demonstrably cost effective. Inadequate personnel training and development programs in data processing can adversely affect accomplishment of the organization's mission.

Provisions for security of the computer hardware, computer programs, data files, data transmission, input and output material, and personnel, to ascertain whether these matters have been adequately considered should also be reviewed by the auditor. This review should include not only the computer equipment present in the central processing facility but also extend to computer terminals, communications operations, and other peripheral equipment.

In reviewing physical security of computer hardware, the auditor should consider the adequacy of contingency plans for continued processing of critical applications in the event of a disruption of normal data processing functions. This should include provisions for emergency power and hardware backup as well as detailed plans for making use of the backup equipment and transporting personnel, programs, forms, and data files to the alternate processing location. The auditor should also consider the extent to which this contingency plan has been tested to determine the probability of continuing data processing support in the event of a real emergency.

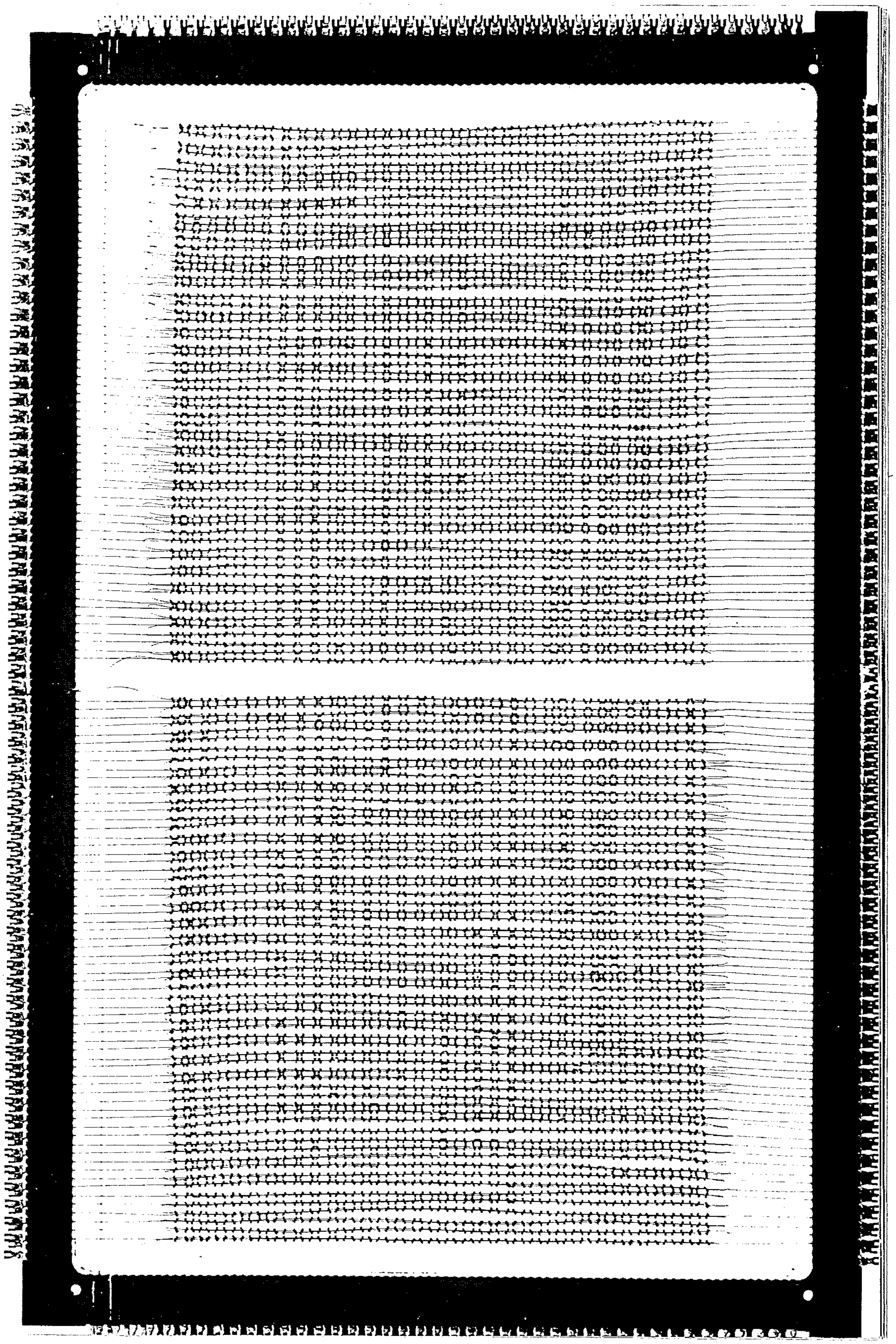
The auditor also needs to review the physical security of data files. This review should insure data and program file libraries are maintained by personnel who do not have access to computers and computer programs, the file libraries are secure, computer operators and other personnel do not have access to the library, and provisions have been made for backup of files (including offsite backup). When files are normally maintained online, the auditor should consider whether these files are protected by adequate access authorization controls and whether backup copies of files are maintained on a regular basis. As a part of the review of procedures for maintaining backup copies of data files, the auditor should verify that backup files are properly identified, labeled, and the contents checked to insured that the backup medium is complete and accurate. Similar stringent controls should exist for program backup files.

Operating Systems Controls

Computer systems are frequently controlled by operating systems (usually referred to as systems software). Since these operating systems provide data handling and multiprograming capabilities, file label checking, and many other authorization controls, the operating system is integral to the general controls over computer processing. The auditor should be aware of the controls the operating system can exercise and should ascertain the extent to which those controls have been implemented, as well as how they may be bypassed or overridden. As a part of this review, the auditor should be aware of the fact that personnel responsible for maintaining the operating system, and other persons with the ability to modify the operating system, may either intentionally or accidentally cause specific control features within the operating system to become ineffective.

Hardware Controls

Computer hardware frequently has designed capabilities for detecting erroneous conditions related to hardware malfunctions (as contrasted to program malfunctions). The auditor should be aware of how (1) the installation relies on these hardware controls, (2) the operating system utilizes these controls, and (3) the detected hardware errors are reported within the installation as well as the procedures for taking corrective action.



Standard for Review of Application Controls in Computer-Based Systems

The third supplemental standard is:

> "The auditor shall review application controls of installed data processing applications to assess their reliability in processing data in a timely, accurate, and complete manner."

Before any assessment of processing reliability or integrity in any application can be complete, both the specific application controls and the general controls must be evaluated in their entirety. While it is possible that an application control weakness could be offset or neutralized by a strong general control, the pervasiveness of a general control weakness may be such that no amount of application controls can assure reliable processing of data.

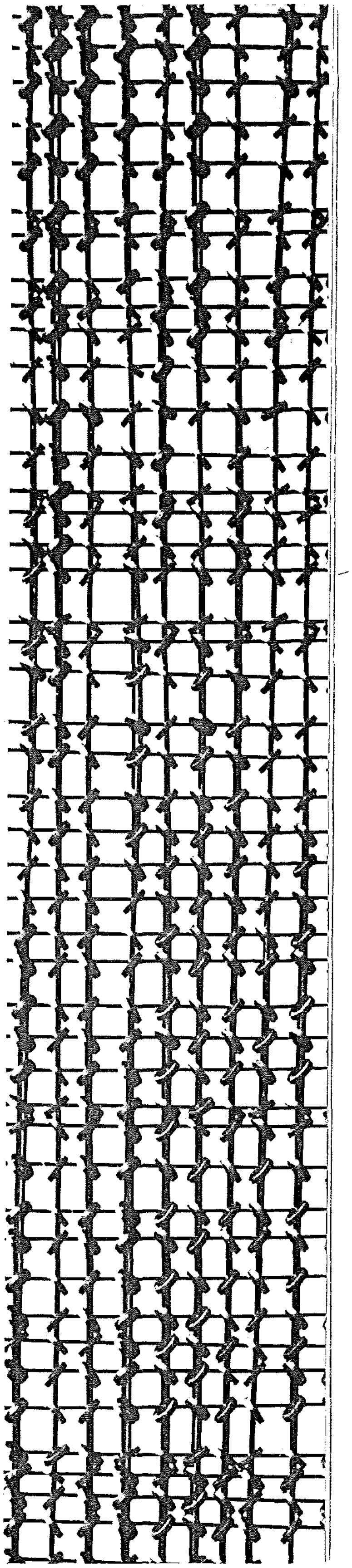
There are two basic objectives to the audit work performed in responding to supplemental standard 3. Both are discussed below.

Conformance with Standards and Approved Design

The first objective is to determine whether the installed application conforms to standards and the latest approved design specifications, and is being efficiently processed.

Audit compliance with supplemental standard 3 provides assurance that the approved specifications, with all built-in internal controls (input, processing, output, etc.,) have been installed as intended, are properly documented, and have been adequately tested.

When the auditor tests data reliability, such tests should include examining supporting documentation for selected transactions, testing the clerical accuracy of the manner in which transactions have been entered and summarized, and testing compliance with control procedures. In addition, auditors may wish to test selected data files to identify possible exception conditions and accuracy of data conversion or capture. If the data records are maintained in machine-readable condition the auditor should, where appropriate, make use of computer-assisted audit techniques in testing data records.



Tests for Control Weaknesses

The second objective is to disclose possible weaknesses in the installed application through periodic audits designed to test internal controls and the reliability of the data produced.

These periodic audits should probe the installed application for weaknesses, changed circumstances which affect risk exposure, etc., with the intention of stimulating corrective modifications and improving the installed applications. Also, the auditor must be mindful, when conducting periodic tests, that there are no guarantees that the application system will continue to operate in accordance with the latest approved specifications. Therefore, adequacy of controls over program changes and operating procedures are most important.

Finally, the auditor must be alert to the possibility of fraud or other irregularities in computer systems. Although auditing for fraud is usually not the primary objective of audits, the detection of fraud should be a general audit objective.

☆ U.S. GOVERNMENT PRINTING OFFICE : 1979 O—288-477