The evolution of IT auditing and internal control standards in financial statement audits

The case of the United States

David C. Yang and Liming Guan
College of Business Administration, University of Hawaii at Manoa, Honolulu, Hawaii, USA

Keywords *Technology led strategy, Auditing, Auditing standards, United States of America*

Abstract *The rapid escalation of technology and the use of computers in business practice result in more information technology (IT) auditing and internal control standards and guidelines to assist auditors in their roles and responsibilities. Several organizations, such as the American Institute of Certified Public Accountants (AICPA), the International Federation of Accountants and the Information Systems Audit and Control Association (ISACA), have issued standards in this area to be observed by their members in performing an IT audit. This paper traces the evolution of US IT auditing and internal control standards in financial statement audits and discusses their significance for the auditing profession. We primarily focus on the discussion of the IT audit standards issued by the AICPA and ISACA. As the use of computers in business data processing gets more widespread and the integration of IT in business processes gets more intricate, we expect to see more pronouncements of IT audit standards in the future. Auditors should well understand these pronouncements, standards and guidelines when performing an IT audit.*

1. Introduction

The computer is one of the most dominant advances of the twentieth century. It has had a tremendous impact on many areas of human activity, including engineering, medicine, science and business. Information technology (IT) or electronic data processing (EDP) has changed the way many organizations conduct business[1]. In fact, IT is one of the major technological advances in business in the last 40 years. IT systems can perform many tasks, and management is continually finding new ways to utilize the computer to promote operational efficiency and to aid in decision making.

Because many businesses at present use computers to process their transactions, the auditing profession has been faced with a need to provide increased guidance for audits conducted in an IT environment. Various authoritative bodies, such as the American Institute of Certified Public Accountants (AICPA), the International Federation of Accountants (IFAC) and the Information Systems Audit and Control Association (ISACA), have issued standards in this area. This paper surveys various US IT auditing and internal control standards in financial statement audits and discusses their significance for the auditing profession. The following list summarizes all the relevant standards in the USA:

Managerial Auditing Journal
Vol. 19 No. 4, 2004
pp. 544-555

0268-6902
DOI 10.1108/02686900410530547

The authors are grateful to Dr Gerald Vinten for his helpful comments on the earlier versions of this paper.

(1) AICPA standards:
- Statement on Auditing Standards (SAS) No. 3 (AICPA, 1974).
- SAS No. 48 (AICPA, 1984).
- SAS No. 94 (AICPA, 2001).

(2) ISACA standards (effective from July 1997):
- Standards for Information Systems Auditing (SISA) 010 (ISACA, 1997a).
- SISA 020 (ISACA, 1997b).
- SISA 030 (ISACA, 1997c).
- SISA 040 (ISACA, 1997d).
- SISA 050 (ISACA, 1997e).
- SISA 060 (ISACA, 1997f).
- SISA 070 (ISACA, 1997g).
- SISA 080 (ISACA, 1997h).

Sections 2 and 3 discuss these standards in detail, and Section 4 concludes the paper.

2. AICPA standards

SASs are issued by the Auditing Standards Board (ASB), the senior technical body of AICPA designated to issue pronouncements on auditing matters. The ASB was formed in October 1978 and is responsible for the development and promulgation of auditing standards and procedures to be observed by members of the AICPA. The AICPA code of professional conduct requires an AICPA member who performs an audit (the auditor) to comply with the standards promulgated by the ASB. The auditor should have sufficient knowledge of the SASs to identify those that are applicable to his/her audit and should be prepared to justify departures. This section surveys the following three SASs that are related directly to an IT audit: SAS No. 3, SAS No. 48, and SAS No. 94.

2.1 SAS No. 3, The effects of IT on the auditor's study and evaluation of internal control

Although computers have not in any significant way changed or established accounting theory as it relates to the type of data to be collected or the manner in which such data should be organized for reporting purposes, computers have substantially altered the methods by which that theory is put into practice (Jancura and Lilly, 1977)[2]. With the increased use of computers in data processing in the US business entities since the mid-1960s, there appeared to be a need for the auditing standard-setters to develop a framework concerning auditing procedures in examining the financial statements of entities that use IT in accounting applications.

In 1974, the auditing standards executive committee of the AICPA issued the SAS No. 3, "The effects of EDP on the auditor's study and evaluation of internal control". It was a first bold step in defining the auditing standards for IT systems (Jancura and Lilly, 1977). The statement provided guidance for audits conducted in IT environments and required auditors to evaluate computers during their audit. According to SAS No. 3, the objectives of accounting control are the same in both a manual system and an IT system. However, the organization and procedures required to accomplish these objectives may be influenced by the method of data processing used. Therefore, the procedures used by an auditor in his/her study and the evaluation of accounting

control to determine the nature, timing, and extent of audit procedures to be applied in the examination of financial statements may be affected. When IT is used in significant accounting applications, the auditor should consider the IT activity in his/her study and evaluation of accounting control. The auditor should consider whether the use of IT in accounting applications is limited or extensive, and whether the IT operations are under the direction of the client or a third party.

SAS No. 1, "The auditor's study and evaluation of internal control", was issued in 1973 (AICPA, 1973). It defines internal control in terms of administrative control and accounting control, and concludes that administrative control is not within the scope of the study and evaluation of internal control contemplated by Generally Accepted Auditing Standards (GAAS). SAS No. 3 was mainly concerned with the unique control aspects that are present if a significant part of the client's financial records are processed in an IT system. In SAS No. 3, IT controls were classified into general and application controls, which the auditor should assess. These control features are tabulated by Wilkinson (1991) and are shown in Table I.

However, as indicated in its title, SAS No. 3 concerned itself with the unique control aspects that were present if a significant portion of an entity's financial records were processed by computers. Since the issuance of SAS No. 3, several events have occurred which had made it inadequate. First, an increasing number of businesses were using complex computer systems as a cost-effective way to process accounting data. Second, many businesses had begun to use interactive systems in which the accounting record keeping and decision-making functions are closely tied. Because of these events, it became more difficult to audit "around the computer", as sound inferences could not be drawn concerning how the processing programs handle erroneous data (Nunter and Ratcliffe, 1985). Many times, the IT function permeated the company's entire accounting process. Therefore, the auditor should not limit his/her attention to only the internal control aspects of the IT function.

Since it was no longer adequate for auditors to limit their focus to the internal control aspects of IT, the ASB of the AICPA issued SAS No. 48, "The effects of computer processing on the examination of financial statements", in July 1984. This statement superseded SAS No. 3, and was broader and more appropriate for auditing needs for financial statements at that time.

Accounting controls	Application controls	Input controls Processing controls Output controls
	General controls	Asset accountability controls Security measures controls Organizational controls Authorization controls Documentation controls Operational controls Management practice controls
Administrative controls		

Source: Based on Wilkinson (1991)

Table I.
Categories of internal controls and security measures

2.2 SAS No. 48, The effects of computer processing on the examination of financial statements

SAS No. 48, "The effects of computer processing on the examination of financial statements," superseded SAS No. 3. It was effective for the examination of financial statements for periods beginning after 31 August 1984. It also amended SAS No. 22 on "Planning and supervision" (AICPA, 1978a), SAS No. 23 on "Analytical review procedures" (AICPA, 1978b), SAS No. 1, Section 320 on "The auditor's study and evaluation of internal control" (AICPA, 1973), and SAS No. 31 on "Evidential matter" (AICPA, 1980) to include additional guidance for audits of financial statements in IT environments.

The ASB felt that auditors should consider the methods of data processing used by the client, including the use of computers, in essentially the same way and at the same time that they consider other significant factors that could affect the audit. The use of IT could affect the nature, timing and extent of audit procedures, so the auditor should consider these effects throughout the audit. Therefore, the ASB felt that guidance concerning the effect of computer processing on audits of financial statements should be integrated with existing guidance rather than presented separately. This is the primary reason why SAS No. 48 amended so many other existing statements.

2.2.1 Planning and supervision. In the GAAS, the first standard of fieldwork, SAS No. 22, requires the work in an audit engagement to be adequately planned, and assistance, if any, to be properly supervised. SAS No. 22, "Planning and supervision", provided guidance for the auditor making an examination in accordance with GAAS. The engagement must be adequately planned and supervised for the auditor to achieve the objectives of the examination, which is to gather the appropriate amount of sufficient competent evidential matter to form the basis for an audit opinion on the financial statements. Part of the planning includes the development of an overall strategy for the expected conduct and scope of the examination. SAS No. 48 adds further planning considerations to those already required by SAS No. 22. It requires the auditor to consider the methods (manual or computerized) used by the client in processing significant accounting information. It also requires the auditor to consider whether it will be necessary to obtain the aid of a specialist in making this determination.

The determination of whether a specialist is needed to evaluate the effects of computer processing and to design the audit tests must be made early in the engagement. The auditor must decide whether he/she or his/her staff has the necessary skills to determine the effect of IT on the audit function. If a specialist is needed, the auditor can choose a computer specialist who is a member of the auditor's firm or an outside specialist. SAS No. 48 says that in either case the computer specialist is considered as a member of the audit team. Therefore, SAS No. 11, "Using the work of a specialist" is inapplicable, since it applies to specialists who are not considered as members of the audit team. Since the computer specialist is a member of the audit team, the auditor is responsible for supervising and evaluating the specialist's work and ascertaining whether the specialist has achieved his/her objectives. This means that the auditor must have a high enough level of computer skills in order to communicate his/her objectives to the specialist, determine that the specialist's procedures will satisfy the auditor's requirements, and evaluate the results of the procedures performed by the specialist and their effect on the timing and nature of the audit procedures to be used.

As mentioned earlier, the auditor is required to consider the methods that the client uses to process accounting information in planning the audit, since this may influence the design of the accounting system and the nature of internal accounting control procedures. The auditor should consider the following factors:

- the extent to which the computer is used in each significant accounting application;
- the complexity of the entity's computer operations, including the use of an outside service center;
- the organizational structure of the computer processing activities;
- the availability of data, since some data may exist only for a short period or only in a computer-readable form, and since input forms may not exist; and
- the use of computer-assisted audit techniques to increase the efficiency of performing audit procedures.

2.2.2 Study and evaluation of internal control. The second standard of fieldwork requires that the auditor study and undertake an evaluation of the client's internal control structure. This is done after the auditor has completed the planning of the audit engagement. The primary guidance for conducting the study and the evaluation of internal control is found in SAS No. 55, "Consideration of the internal control structure in a financial statement audit" (AICPA, 1988a) issued in April 1988. SAS No. 55 supersedes SAS No. 1, Section 320, "The auditor's study and evaluation of internal control". Although SAS No. 55 would not be effective for audits of financial statements for periods beginning on 1 January 1990, early application of the provisions of the statement was permissible.

Section 320 of SAS No. 1 defines internal control in terms of administrative and accounting control. SAS No. 3 is intended to read in conjunction with Section 320 of SAS No. 1. In SAS No. 3, internal accounting control procedures can be separated into two categories (general control and application control procedures) when computer processing is used for significant accounting applications. The objectives of the system of internal accounting control and the objectives of the auditor's review of the system are the same for both manual and computerized systems. However, when reviewing the controls, the auditor may find it more efficient to first review the general controls affecting an application control before reviewing a specific application control, since the effectiveness of the application control is dependent on the adequacy of the general control.

In conducting the study and evaluation of the internal accounting control system, in order to place reliance on the system, the auditor will need to do the following:

- undertake a preliminary review of the system (obtain a general understanding of the flow of transactions and assess the control environment);
- complete the system review (obtain a detailed understanding of the prescribed general and application controls and document that understanding);
- conduct compliance tests;
- evaluate the results.

These same steps are performed in both manual and computerized systems, but the procedures applied will be different.

Since different procedures will be used in an IT environment, SAS No. 48 highlights the distinguishing characteristics of IT systems that should be considered by the auditor when conducting his/her study and evaluation. These characteristics are:

- transaction trails may exist for only a short time, or only in computer-readable form;
- computer processing of information essentially eliminates the clerical errors, but programming errors may exist;
- computer processing systems may integrate internal control functions that are normally segregated in manual systems;
- ease of unauthorized access to data (as well as assets) is sometimes enhanced with computerized systems;
- computer systems provide increased management tools that are useful in supervising and reviewing company operations;
- computer systems may allow automatic initiation or execution of certain transactions; and
- output from computer processing may be used in performing manual control procedures such that automated and manual controls become interdependent.

Some of the characteristics listed above strengthen the internal control system relative to manual systems, while others may weaken it. Therefore, the auditor should concentrate his/her study and evaluation on areas where incompatible functions may be performed.

If the IT system processes transactions and provides information that are used to reconcile the records to the physical assets, those responsible for the computer processing should not be involved in the reconciliation process. The auditor is limited to using observation and inquiry procedures when conducting compliance tests of the segregation of duties. There may be other procedures available for compliance tests of other aspects. In any case, the auditor should plan the testing so that he/she is reasonably sure that such control procedures are actually performed by the client throughout the year and that the programs are those that are actually used by the client.

It should be noted, however, that SAS No. 55 does not supersede or amend SAS No. 48. The paragraphs in SAS No. 48 that amend SAS No. 1, Section 320 would, therefore, stand as of today.

2.2.3 Evidential matter. Once the auditor completes the study and evaluation of internal controls, substantive testing must be performed to obtain sufficient, competent evidential matter on which the auditor can base his/her opinion. SAS No. 48 states that audit evidence is not affected by computer processing, but the methods used to gather audit evidence may be affected. In an IT environment, the auditor may have to use computer-assisted audit techniques such as computer-aided tracing and mapping, audit software, and embedded audit data collection to gather evidence. The auditor will have to rely more heavily on computer-assisted audit methods for inspection and analytical review procedures.

2.2.4 Analytical review procedures. The use of analytical review procedures was covered by SAS No. 23, "Analytical review procedures", which was later on superseded by SAS No. 56, "Analytical procedures" (AICPA, 1988b), issued in April 1988. SAS No. 56 provides guidance on the use of analytical procedures and requires the use of analytical procedures in the planning and overall review of all audits. When the client

has an IT system, the auditor must consider a particular factor in determining the usefulness of such procedures. This factor relates to the increased availability of data prepared for management's use when computer processing is used. In many cases, management may establish programs that use information from the financial records to aid them in making administrative decisions. In this situation, there may be an increased amount of data prepared for management's use, but also may be used by the auditor in conducting the analytical review procedures. This may allow the auditor to conduct many tests that cannot be performed easily in manual systems.

2.2.5 Qualifications of the audit team. The first GAAS required individuals to have adequate technical training and proficiency as an auditor. Since the use of computers was so widespread, SAS No. 48 required auditors to be trained and professionally competent in the use of computers. The auditor should have a basic understanding of computers, computer facility organization, computer data-processing methods, computer processing controls, and computer-assisted audit techniques. AICPA (1984) has recommended that the auditor should think about whether specialized skills are needed to consider the effect of computer processing on the audit, to understand the flow of transactions, to understand the nature of internal accounting control procedures, or to design and perform audit procedures. If specialized skills are needed, the auditor should seek the assistance of a professional possessing such skills, who may be either on the auditor's staff or an outside professional.

Lastly, to provide for more specific guidelines to meet the objectives of the auditor's study of internal control in IT systems, the AICPA issue audit and accounting guides to present recommendations as to the auditing procedures. These include "The auditor's study and evaluation of internal control in EDP systems" and "Computer-assisted audit techniques", both prepared by the Computer Services Executive Committee of the AICPA. Although these two guides were issued prior to SAS No. 48's superseding SAS No. 3, they are still valid supplements. Both state as a "Notice to readers" that what is contained within are merely suggestions or recommendations on auditing procedures and are not intended to suggest preferable practices. Yet, they go on to state that "although it does not have the authority of a pronouncement by that board (ASB), AICPA members may have to justify departure from the auditing procedures contained in this guide if their work is challenged".

2.3 SAS No. 94, The effect of IT on the auditor's consideration of internal control in a financial statement audit

AICPA (2001) released SAS No. 94, "The effect of IT on the auditor's consideration of internal control in a financial statement audit," effective for audits of financial statements for periods beginning on or after 1 June 2001, with earlier application being permissible. SAS No. 94 provided guidance to auditors about the effect of IT on internal control, and on the auditors' understanding of internal control and assessment of control risk. SAS No. 94 amended SAS No. 55, "Consideration of internal control in a financial statement audit" (AICPA, 1988a).

SAS No. 94 was intended to apply to audits of all sizes of business. It was not intended only for very large organizations with sophisticated IT systems, because the impact of IT on internal control is related more to the nature and complexity of the systems in use rather than to the entity's size. The five most significant aspects of No. 94 identified by Tucker (2001) are discussed below.

2.3.1 How IT affects internal control. Internal control is also referred to as internal control structure. In obtaining an understanding of internal control sufficient to plan the audit, the auditor should consider how an entity's use of IT and manual procedures might affect controls that are relevant to the audit. The auditor then assesses control risk for the assertions embodied in the account balance, transaction class, and disclosure components of the financial statements.

Internal control consists of five interrelated components: the control environment, risk assessment, control activities, information and communication, and monitoring. SAS No. 94 points out that an entity's IT use may affect any of these components. For example, an entity may use IT as part of discrete systems that support only particular business units, functions, or activities, such as a unique accounts receivable system for a particular business unit or a system that controls the operation of factory equipment. Alternatively, an entity may have complex, highly integrated systems that share data and are used to support all aspects of the entity's financial reporting, operations, and compliance objectives.

The use of IT may also affect how businesses initiate, record, process and report transactions. Controls in systems that use IT consist of a combination of automated controls (e.g. controls embedded in computer programs) and manual controls. However, manual controls may be independent of IT, may use information produced by IT, or may be limited to monitoring the effective functioning of IT and of automated controls, and to handling exceptions. Thus, an entity's mix of manual and automated controls should vary with the nature and complexity of the entity's use of IT.

Since the use of IT can generate benefits and meanwhile post risks to an entity's internal control, the auditor should expect to encounter IT systems and electronic records rather than paper-based documents.

2.3.2 The auditor's consideration of IT. SAS No. 94 does not change SAS No. 55's requirement that the auditor obtain a sufficient understanding of internal control to plan the audit. However, it expands the concept from SAS No. 80, "Amendment to statement on auditing standards No. 31, evidential matter", that in circumstances where a significant amount of information supporting one or more financial statement assertions is electronically initiated, recorded, processed, and reported, the auditor may determine that it is not practical or possible to restrict detection risk to an acceptable level by performing only substantive tests for one or more financial statement assertions. In such circumstances, the auditor should obtain evidential matter about the effectiveness of both design and operation of controls to reduce the assessed level of control risk.

The statement provides two situations where the auditor may find it impractical to design effective substantive tests that by him/her would provide sufficient evidence that certain assertions are not materially misstated. One situation occurs when an entity conducts business using IT to initiate orders for goods based on predetermined decision rules. In this situation, the entity also pays the related payables based on system-generated information regarding receipt of goods, while no other documentation of orders or goods received is produced or maintained. The other situation is when an entity provides electronic services to customers and uses IT to log services provided to users, initiate bills for the services, process the billing transactions, and automatically record such amounts in electronic accounting records. Thus, if the auditor plans to perform only substantive tests, he/she needs to be satisfied that such an approach will be effective.

2.3.3 Performing tests of controls. Tests of controls refer to the procedures directed toward either the effectiveness of the design or operation of a control. In designing tests of automated controls, the auditor may need to obtain supporting evidence that the operation of controls directly related to the assertions and other indirect controls on which these controls depend, is effective. The extent of testing of an automated control may be reduced due to the inherent consistency of IT processing. After determining that an automated control is functioning as intended, the auditor should consider performing tests to ensure that the control continues to function effectively.

The techniques used by the auditor to test automated controls may be different from those that are used to test manual controls. The auditor may also need to use other automated tools or reports produced by IT to test the operating effectiveness of general controls, access controls, and system software controls. Finally, the auditor should consider whether specialized skills are needed to design and perform such tests of controls.

2.3.4 Specialized skills. SAS No. 94 provides guidelines to help auditors to determine whether specialized skills are needed to consider the effect of IT on the audit, to understand the controls, or to design and perform audit procedures. The statement also includes several factors that the auditor should consider in determining whether a professional possessing the IT skills is needed on the audit team, as well as the procedures that the professional should perform once such need is determined. The auditor who uses a professional with IT skills should follow the guidance in SAS No. 22, "Planning and supervision", as amended by SAS No. 48, "The effects of computer processing on the audit of financial statements". As a member of the audit team, the professional with IT skills requires the same degree of supervision and review as any other assistant.

2.3.5 The financial reporting process. SAS No. 55 had required the auditor to "obtain sufficient knowledge of the information system" to understand "the financial reporting process used to prepare the entity's financial statements, including significant accounting estimates and disclosures". However, the statement did not specify which aspects of the financial reporting process the auditor should understand.

SAS No. 94 clarifies what the auditor should know to understand the automated and manual procedures an entity uses to prepare its financial statements and related disclosures. The understanding includes the following procedures an entity uses to:

- enter transaction totals into the general ledger;
- initiate, record, and process journal entries in the general ledger, including standard journal entries required on a recurring basis and non-standard journal entries to record non-recurring or unusual transactions or adjustments; and
- record recurring and non-recurring adjustments to the financial statements that are not reflected in formal journal entries, such as consolidating adjustments, report combinations, and reclassifications.

Overall, SAS No. 94 moves the professional literature forward by recognizing the types of systems, controls and evidence auditors encounter at present. It is an important step in a process to acknowledge IT in auditing standards.

Other authoritative bodies have issued guidelines and pronouncements that are similar to those issued by the AICPA in regard to auditing in IT environments. The next section describes the standards and guidelines provided by ISACA.

3. ISACA standards

Founded in 1969, ISACA, named EDP Auditors Association previously, sponsors international conferences, training events and a global knowledge network (K-NET), administers the globally respected Certified Information Systems Auditor™ (CISA®) designation and the new Certified Information Security Manager™ (CISM™) designation, and develops globally applicable information systems (IS) auditing and control standards. The Standards Board of ISACA issues the SISA, which define mandatory requirements for IS auditing and reporting. These standards are to be observed by the holders of CISA®. A total of eight standards have been issued to date, effective for all IS audits with periods of coverage beginning on 25 July 1997.

3.1 SISA 010, Audit charter

This standard requires that the responsibility, authority and accountability of the IS audit function appropriately be documented in an audit charter or engagement letter.

3.2 SISA 020, Independence

This standard provides guidance on professional independence, requiring that in all matters related to auditing, the IS auditor is to be independent of the auditee in attitude and appearance. It also requires that the IS audit function be sufficiently independent of the area being audited to permit objective completion of the audit.

3.3 SISA 030, Professional ethics and standards

Under this standard, the auditor should adhere to the Code of Professional Ethics of the ISACA. Due professional care and observance of applicable professional auditing standards are also to be exercised in all aspects of the IS auditor's work.

3.4 SISA 040, Competence

This standard requires that the IS auditor is to be technically competent, having the skills and knowledge necessary to perform the auditor's work. It also requires that the auditor maintain technical competence through appropriate continuing professional education.

3.5 SISA 050, Planning

Under SISA 050, the IS auditor is required to plan the audit work to address the audit objectives and to comply with applicable professional auditing standards.

3.6 SISA 060, Performance of audit work

This standard requires that IS audit staff be appropriately supervised to provide assurance that audit objectives are accomplished and applicable professional auditing standards are met. During the course of the audit, the IS auditor is required to obtain sufficient, reliable, relevant and useful evidence to achieve the audit objectives effectively. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence.

3.7 SISA 070, Reporting

Under this standard, the auditor is required to provide a report, in appropriate form, to intended recipients upon the completion of audit work. In the audit report, the auditor should state the scope, objectives, period of coverage, and the nature and extent of the

audit work performed. The report should also identify the organization, the intended recipients and any restrictions on circulation. Finally, the report should state the findings, conclusions and recommendations and any reservations or qualifications that the auditor has with respect to the audit.

3.8 SISA 080, Follow-up activities

During the follow-up activities, the auditor should request and evaluate appropriate information on previous relevant findings, conclusions and recommendations to determine whether appropriate actions have been implemented in a timely manner.

The ISACA is currently considering the following topics to be addressed in future standards, guidelines and procedures: business-to-business e-commerce reviews, business intelligence, business process re-engineering, capacity review, communication scenarios, computer forensics, customer relationship management, data mining, and disaster recovery planning review, among others.

4. Conclusions

Since the use of computers in data processing has become so widespread, auditors have had to deal with conducting audits in IT environments. Although the overall audit objectives are not different for a computerized system, the methods and procedures that the auditor uses in conducting the audit are different. Therefore, various authoritative bodies in the United States have issued pronouncements and guidelines to aid the auditor in conducting his/her examination of financial statements in an IT environment. The trend will continue well into the future and we can expect to see more pronouncements in this area, and auditors should understand well these pronouncements, standards and guidelines.

Notes

1. In standards and guidelines issued by various organizations, the term EDP is used interchangeably with computer information systems (CIS) and information systems (IS).
2. The introduction of data processing equipment has many impacts on the traditional manual accounting systems. For example, the EDP requires that the recording and processing functions be concentrated in departments that are separate from the origin of the data. Computerization has also reduced substantially the time available for the review of transactions before their entry into the accounting records. As a result, in poorly controlled systems the opportunity for discovering errors before they have an impact on operations has been reduced, which leads to the increased importance of internal control procedures. Finally, computerization could potentially eliminate the audit trails by which individual records can be traced to final reports or to the original transaction.

References

AICPA (1973), *Statement on Auditing Standards No. 1, Section 320: The Auditor's Study and Evaluation of Internal Control*, New York, NY.

AICPA (1974), *Statement on Auditing Standards No. 3: The Effects of EDP on the Auditor's Study and Evaluation of Internal Control*, New York, NY.

AICPA (1978a), *Statement on Auditing Standards No. 22: Planning and Supervision*, New York, NY.

AICPA (1978b), *Statement on Auditing Standards No. 23: Analytical Review Procedures*, New York, NY.

AICPA (1980), *Statement on Auditing Standards No. 31: Evidential Matter*, New York, NY.

AICPA (1984), *Statement on Auditing Standards No. 48: The Effects of Computer Processing on the Examination of Financial Statements*, New York, NY.

AICPA (1988a), *Statement on Auditing Standards No. 55: Consideration of the Internal Control Structure in a Financial Statement Audit*, New York, NY.

AICPA (1988b), *Statement on Auditing Standards No. 56: Analytical Procedures*, New York, NY.

AICPA (2001), *Statement on Auditing Standards No. 94: The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit*, New York, NY.

ISACA (1997a), *Standards for Information Systems Auditing 010: Audit Charter*, Rolling Meadows, IL.

ISACA (1997b), *Standards for Information Systems Auditing 020: Independence*, Rolling Meadows, IL.

ISACA (1997c), *Standards for Information Systems Auditing 030: Professional Ethics and Standards*, Rolling Meadows, IL.

ISACA (1997d), *Standards for Information Systems Auditing 040: Competence*, Rolling Meadows, IL.

ISACA (1997e), *Standards for Information Systems Auditing 050: Planning*, Rolling Meadows, IL.

ISACA (1997f), *Standards for Information Systems Auditing 060: Performance of Audit Work*, Rolling Meadows, IL.

ISACA (1997g), *Standards for Information Systems Auditing 070: Reporting*, Rolling Meadows, IL.

ISACA (1997h), *Standards for Information Systems Auditing 080: Follow-up Activities*, Rolling Meadows, IL

Jancura, E. and Lilly, F. (1977), "SAS No. 3 and the evaluation of internal control", *Journal of Accountancy*, pp. 69-74.

Nunter, P. and Ratcliffe, T. (1985), "Impact of computer processing on financial audits", *The CPA Journal*, pp. 34-8.

Tucker, G. (2001), "IT and audit", *Journal of Accountancy*, pp. 41-3.

Wilkinson, J.W. (1991), *Accounting and Information Systems*, Wiley, New York, NY, p. 193.

Further reading

AICPA (1977), "The auditor's study and evaluation of internal control in EDP systems", The Computer Services Executive Committee, New York, NY.

AICPA (1979), "Computer-assisted audit techniques", The Computer Services Executive Committee, New York, NY.