STATEMENT OF AUDITING STANDARDS
310
AUDITING IN A COMPUTER INFORMATION SYSTEMS ENVIRONMENT

(Issued January 1997; revised January 2004)

Contents *Paragraphs*

This SAS remains in effect for audits of financial statements for periods beginning before 15 December 2004. For audits of financial statements for periods beginning on or after 15 December 2004, the new SAS 315 and SAS 330 are applicable. Early application of the provisions of SAS 315 and SAS 330 is permissible.

STATEMENT OF AUDITING STANDARDS
310
AUDITING IN A COMPUTER INFORMATION SYSTEMS ENVIRONMENT

Statements of Auditing Standards (SASs) are to be read in the light of SAS 010 "The scope and authority of auditing pronouncements". In particular, they contain basic principles and essential procedures, (auditing standards), indicated by paragraphs in ***bold italic type****, with which auditors are required to comply in the conduct of any audit including those of companies applying section 141D of the Companies Ordinance. SASs also include explanatory and other material which is designed to assist auditors in interpreting and applying auditing standards.*

Introduction

1. The purpose of this Statement of Auditing Standards (SAS) is to establish standards and provide guidance on procedures to be followed when an audit is conducted in a computer information systems (CIS) environment. For purposes of SASs, a CIS environment exists when a computer of any type or size is involved in the processing by the entity of financial information of significance to the audit, whether that computer is operated by the entity or by a third party.

2. The auditors should consider how a CIS environment affects the audit. (SAS 310.1)

3. The overall objective and scope of an audit does not change in a CIS environment. However, the use of a computer changes the processing, storage and communication of financial information and may affect the accounting and internal control systems employed by the entity. Accordingly, a CIS environment may affect:

   a. the procedures followed by the auditors in obtaining a sufficient understanding of the accounting and internal control systems;

   b. the consideration of inherent risk and control risk through which the auditors arrive at the risk assessment; and

   c. the auditors' design and performance of tests of control and substantive procedures appropriate to meet the audit objective.

Skills and competence

4. The auditors should have sufficient knowledge of the CIS to plan, direct, supervise and review the work performed. The auditors should consider whether specialised CIS skills are needed in an audit. (SAS 310.2)

5. These may be needed to:

   a. obtain a sufficient understanding of the accounting and internal control systems affected by the CIS environment;

   b. determine the effect of the CIS environment on the assessment of overall risk and of risk at the account balance and class of transactions level; and

   c. design and perform appropriate tests of control and substantive procedures.

   If specialised skills are needed, the auditors would seek the assistance of a professional possessing such skills, who may be either the auditors' staff or an outside professional.

6. If the use of such a professional is planned, the auditors should obtain sufficient appropriate audit evidence that such work is adequate for the purposes of the audit, in accordance with SAS 520 "Using the work of an expert". (SAS 310.3)

Planning

7. In accordance with SAS 300 "Audit risk assessments and accounting and internal control systems" the auditors should obtain an understanding of the accounting and internal control systems sufficient to plan the audit and develop an effective audit approach. (SAS 310.4)

8. In planning the portions of the audit which may be affected by the client's CIS environment, the auditors should obtain an understanding of the significance and complexity of the CIS activities and the availability of data for use in the audit. (SAS 310.5)

9. This understanding would include such matters as:

a. the significance and complexity of computer processing in each significant accounting application. Significance relates to materiality of the financial statement assertions affected by the computer processing. An application may be considered to be complex when, for example:

i. the volume of transactions is such that users would find it difficult to identify and correct errors in processing;

ii. the computer automatically generates material transactions or entries directly to another application;

iii. the computer performs complicated computations of financial information and/or automatically generates material transactions or entries that cannot be (or are not) validated independently; and

iv. transactions are exchanged electronically with other organisations (as in electronic data interchange systems) without manual review for propriety or reasonableness;

b. the organisational structure of the client's CIS activities and the extent of concentration or distribution of computer processing throughout the entity, particularly as they may affect segregation of duties; and

c. the availability of data. Source documents, certain computer files, and other evidential matter that may be required by the auditors may exist for only a short period or only in machine-readable form. Client CIS may generate internal reporting that may be useful in performing substantive tests (particularly analytical procedures). The potential for use of computer-assisted audit techniques may permit increased efficiency in the performance of audit procedures, or may enable the auditors to economically apply certain procedures to an entire population of accounts or transactions.

10. When the CIS is significant, the auditors should also obtain an understanding of the CIS environment and whether it may influence the assessment of inherent and control risks. (SAS 310.6)

11. The nature of the risks and the internal control characteristics in CIS environments include the following:

a. Lack of transaction trails

Some CIS are designed so that a complete transaction trail that is useful for audit purposes might exist for only a short period of time or only in computer readable form. Where a complex application system performs a large number of processing steps, there may not be a complete trail. Accordingly, errors embedded in an application's programme logic may be difficult to detect on a timely basis by manual (user) procedures.

b. Uniform processing of transactions

Computer processing uniformly processes like transactions with the same processing instructions. Thus, the clerical errors ordinarily associated with manual processing are virtually eliminated. Conversely, programming errors (or other systematic errors in hardware or software) ordinarily result in all transactions being processed incorrectly.

c. Lack of segregation of functions

Many control procedures that would ordinarily be performed by separate individuals in manual systems may be concentrated in CIS. Thus, an individual who has access to computer programme, processing or data may be in a position to perform incompatible functions.

d. Potential for errors and irregularities

The potential for human error in the development, maintenance and execution of CIS may be greater than in manual systems, partially because of the level of detail inherent in these activities. Also, the potential for individuals to gain unauthorised access to data or to alter data without visible evidence may be greater in CIS than in manual systems. In addition, decreased human involvement in handling transactions processed by CIS can reduce the potential for observing errors and irregularities. Errors or irregularities occurring during the design or modification of application programme or systems software can remain undetected for long periods of time.

e. Initiation or execution of transactions

CIS may include the capability to initiate or cause the execution of certain types of transactions automatically. The authorisation of these transactions or procedures may not be documented in the same way as those in a manual system, and management's authorisation of these transactions may be implicit in its acceptance of the design of the CIS and subsequent modification.

f. Dependence of other controls over computer processing

Computer processing may produce reports and other output that are used in performing manual control procedures. The effectiveness of these manual control procedures can be dependent on the effectiveness of controls over the completeness and accuracy of computer processing.

In turn, the effectiveness and consistent operation of transaction processing controls in computer applications is often dependent on the effectiveness of general CIS controls.

g. Potential for increased management supervision

CIS can offer management a variety of analytical tools that may be used to review and supervise the operations of the entity. The availability of these additional controls, if used, may serve to enhance the entire internal control structure.

h. Potential for the use of computer-assisted audit techniques

The case of processing and analysing large quantities of data using computers may provide the auditors with opportunities to apply general or specialised computer audit techniques and tools in the execution of audit tests.

Both the risks and the controls introduced as a result of these characteristics of CIS have a potential impact on the auditors' assessment of risk, and the nature, timing and extent of audit procedures.

Assessment of risk

12. ***In accordance with SAS 300 "Audit risk assessments and accounting and internal control systems" the auditors should make an assessment of inherent and control risks for material financial statement assertions. (SAS 310.7)***

13. The inherent risk and control risk in a CIS environment may have both a pervasive effect and an account-specific effect on the likelihood of material misstatements, as follows:

a. the risks may result from deficiencies in pervasive CIS activities such as programme development and maintenance, systems software support, operations, physical CIS security, and control over access to special-privilege utility programme. These deficiencies would tend to have a pervasive impact on all application systems that are processed on the computer; and

b. the risks may increase the potential for errors or fraudulent activities in specific applications, in specific data bases or master files, or in specific processing activities. For example, errors are not uncommon in systems that perform complex logic or calculations, or that must deal with many different exception conditions. Systems that control cash disbursements or other liquid assets are susceptible to fraudulent actions by users or by CIS personnel.

14. As new CIS technologies emerge, they are frequently employed by clients to build increasingly complex computer systems that may include micro-to-mainframe links, distributed data bases, end-user processing, and business management systems that feed information directly into the accounting systems. Such systems increase the overall sophistication of CIS and the complexity of the specific applications that they affect. As a result, they may increase risk and require further consideration.

Audit procedures

15. ***In accordance with SAS 300 "Audit risk assessments and accounting and internal control systems", when the CIS is significant, the auditors should consider the CIS environment in designing audit procedures to reduce audit risk to an acceptably low level. (SAS 310.8)***

16. The auditor's specific audit objectives do not change whether accounting data is processed manually or by computer. However, the methods of applying audit procedures to gather evidence may be influenced by the methods of computer processing. The auditors can use either manual audit procedures, computer-assisted audit techniques, or a combination of both to obtain sufficient evidential matter. However, in some accounting systems that use a computer for processing significant applications, it may be difficult or impossible for the auditors to obtain certain data for inspection, enquiry, or conformation without computer assistance.

Compliance with International Standards on Auditing

17. Compliance with the auditing standards contained in this SAS ensures compliance in all material respects with the basic principles and essential procedures in International Standard on Auditing 401 "Auditing in a Computer Information Systems Environment".

Effective date

18. Auditors are required to comply with the requirements of this SAS in respect of audits of financial statements for periods beginning before 15 December 2004.