

Auditing Standard

AUS 214
(October 1995)

Auditing in a CIS Environment

Prepared by the **Auditing Standards Board** of the
Australian Accounting Research Foundation

Issued by the
Australian Accounting Research Foundation
on behalf of the **Australian Society of Certified
Practising Accountants** and **The Institute of
Chartered Accountants in Australia**

The Australian Accounting Research Foundation was established by the Australian Society of Certified Practising Accountants and The Institute of Chartered Accountants in Australia and undertakes a range of technical and research activities on behalf of the accounting profession as a whole. A major responsibility of the Foundation is the development of Australian Auditing Standards and Statements.

Auditing Standards contain the basic principles and essential procedures identified in bold-type (black lettering) which are mandatory, together with related guidance. For further information about the responsibility of members for compliance with AUSs refer Miscellaneous Professional Statement APS 1.1 "Conformity with Auditing Standards".

Copies of this Standard are available for purchase from the offices of the Australian Accounting Research Foundation, 211 Hawthorn Road, Caulfield, Victoria 3162, Australia.

Phone: (03) 9524 3600
Fax: (03) 9523 5499
Email: standard@aarf.asn.au

COPYRIGHT

© 1995 Australian Accounting Research Foundation.

ISSN 1324-4183

AUS 214 "AUDITING IN A CIS ENVIRONMENT"

CONTENTS

	<i>Paragraphs</i>
Introduction.....	.01-.04
Skills and Competence.....	.05-.06
Knowledge of the Business.....	.07-.08
Planning09-.11
Assessment of Risk.....	.12-.18
Audit Procedures.....	.19-.23
Operative Date24
Compatibility with International Standards on Auditing25

AUS 214 "AUDITING IN A CIS ENVIRONMENT"

AUDITING STANDARD

AUS 214 "AUDITING IN A CIS ENVIRONMENT"

Introduction

- .01 The purpose of this Auditing Standard (AUS) is to establish standards and provide guidance regarding auditing in a computer information systems (CIS) environment. For the purposes of AUSs, a CIS environment exists when a computer of any type or size is involved in the processing by an entity of financial information of significance to the audit, whether that computer is operated by the entity or a third party.
- .02 *The auditor should consider how the CIS environment affects the audit.*
- .03 The use of a computer has implications for the processing, storage and communication of financial information, and therefore affects the internal control structure employed by the entity. The CIS environment affects all aspects of the audit including the:
- (a) consideration of inherent risk and control risk;
 - (b) procedures followed by the auditor to obtain a sufficient understanding of the internal control structure; and
 - (c) auditor's design and performance of audit procedures.
- .04 As a component of the internal control structure of an entity, a CIS has a number of roles. Such roles include actually performing controls and providing information to management to assist them in controlling the business. Whereas management will often require reperformance or review of a manual process or control to confirm its integrity and consistency of performance, management tend to assume that a computer system once implemented, works correctly. Thus effective design, testing, implementation and ongoing maintenance of the system are important factors in its integrity.

Skills and Competence

- .05 *The auditor should have sufficient knowledge of the CIS to plan, direct, supervise and review the work performed. The auditor should consider whether specialised CIS skills are needed in an audit.* Specialised CIS skills may be needed to:

AUS 214 "AUDITING IN A CIS ENVIRONMENT"

- (a) determine the effect of the CIS environment on the assessment of overall audit risk and of risk at the account balance and class of transaction levels;
 - (b) obtain an understanding of the internal control structure affected by the CIS environment and its effect on the business operations of the entity; and
 - (c) design and perform appropriate tests of control and substantive procedures; and
 - (d) evaluate the results of procedures performed.
- .06 ***When using the work performed by a CIS expert, the auditor should obtain sufficient appropriate audit evidence that such work will be adequate for the purposes of the audit.*** When using the work of an expert, the auditor would refer to AUS 606 "Using the Work of an Expert".

Knowledge of the Business

- .07 ***The auditor should have or obtain a knowledge of the CIS environment sufficient to enable the auditor to assess its potential impact on the identification and understanding of the events, transactions and practices that, in the auditor's judgement, may have a significant effect on the financial report or audit report. In this regard, the auditor should consider the financial and non-financial aspects of the CIS environment and their implications for the financial report and audit report.***
- .08 Matters the auditor would ordinarily consider in obtaining this knowledge include:
- (a) the entity's use of and attitude towards information technology and the effect of this on the nature and source of systems applications, for example the extent to which the entity purchases recognised and proven systems applications or develops systems applications inhouse or under contract;
 - (b) usage of CIS by the entity compared with general usage within the industry and the local environment within which the entity operates, and information technology trends, including generally available information about CIS usage by competitors and trading partners; and

AUS 214 "AUDITING IN A CIS ENVIRONMENT"

- (c) recent and planned changes to the entity's CIS and CIS environment, for example outsourcing the CIS department, changing the technical platform and changing CIS leadership and business direction.

Planning

- .09 ***In accordance with AUS 402 "Risk Assessments and Internal Controls", the auditor should obtain an understanding of the internal control structure sufficient to plan the audit and develop an effective audit approach.***
- .10 ***In planning the portions of the audit which may be affected by the entity's CIS environment, the auditor should obtain an understanding of the significance and complexity of the CIS activities and the availability of data for use in the audit.*** This understanding would include such matters as:
 - (a) the organisational structure of the entity's CIS activities and the extent of concentration or distribution of computer processing and development throughout the entity, particularly as they may affect segregation of duties at both the user and CIS personnel levels;
 - (b) the significance of computer processing in each significant accounting application. For this purpose significance relates to materiality of the financial report assertions affected by the computer processing;
 - (c) the complexity of computer processing in each significant accounting application. Applications may be considered 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 (integrated systems);
 - (iii) the computer performs complicated computations of financial information and/or automatically generates material transactions or entries that may not be (or are not) validated independently; and

AUS 214 "AUDITING IN A CIS ENVIRONMENT"

- (iv) transactions are exchanged electronically with other organisations (as in electronic data interchange (EDI) systems);
 - (d) plans by the entity to replace or significantly change a CIS where these changes will affect the internal control structure; and
 - (e) the availability of data. Source documents, certain computer files, and other evidential matter that may be required by the auditor may exist for only a short period or only in machine-readable form. An entity's CIS may generate internal reports 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 auditor to economically apply certain procedures to an entire population of accounts or transactions.
- .11 In planning the audit, the auditor designs audit procedures that will provide sufficient appropriate audit evidence. During the initial planning phase of the audit, the auditor needs to assess whether to use computer-assisted audit techniques. The need to process and analyse large quantities of data using computers may provide the auditor with opportunities to apply general or specialised computer-assisted audit techniques and tools in the execution of audit tests. Computer-assisted audit techniques may be used as tests of control or substantive procedures to obtain sufficient appropriate audit evidence.

Assessment of Risk

- .12 *In accordance with AUS 402 "Risk Assessments and Internal Controls", the auditor should make an assessment of inherent and control risks for material financial report assertions.*
- .13 The inherent and control risks in a CIS environment may have both a pervasive and an account-specific effect on the likelihood of material misstatement:
- (a) the risks may result from deficiencies in pervasive CIS activities such as program development and maintenance, systems software support, operations, physical CIS security, and control over access to special-privilege utility programs. These deficiencies would tend to have a

AUS 214 "AUDITING IN A CIS ENVIRONMENT"

- pervasive effect 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 databases or master files, or in specific processing activities. For example errors are not uncommon in systems that perform complex logic tasks or calculations, or that must deal with many different exception conditions. Systems that control cash disbursements or other liquid assets are more susceptible to fraudulent actions.
- .14 In making the assessment of inherent and control risks, the auditor would consider such matters as the extent to which:
- (a) the client develops and operates their own applications rather than outsourcing and the use of established industry and financial packages;
 - (b) aspects of the entity's industry or internal environment may affect the development and application of controls. For example competitive pressure to introduce EDI may result in the entity using a CIS that is not adequately controlled or performing in accordance with specifications;
 - (c) the users have or can grant access to specific functions or data;
 - (d) users have the ability to change data and develop reports (for example to change data or formulae on spreadsheets);
 - (e) pervasive CIS controls (such as systems development and program maintenance, and control over users' access to sensitive functions) affect the reliability of all application systems that are processed on the computer. The impact of these controls is dependent on both the extent to which they apply to specific applications (for example whether the aspects of the systems in which the auditor has an interest are developed and controlled centrally) and the extent to which the quality of the controls is appropriate to the level of risk associated with that application (or the aspect of the application in which the auditor has an interest);
 - (f) the nature and extent of documentation regarding the CIS is appropriate given the complexity of, and inherent risks faced by the CIS environment;

AUS 214 "AUDITING IN A CIS ENVIRONMENT"

- (g) factors that affect the quality of audit evidence available, for example a paperless environment, may increase the potential for audit evidence to be incomplete, unreliable or difficult to obtain;
 - (h) specific risks associated with a particular CIS environment are identified, for example electronic funds transfer systems where the risk of irregularities may be increased or a complex CIS environment where the risk of error may be higher;
 - (i) end-user computing, which refers to any individual exercising control over and using a particular resource or more particularly a software application, is used to produce financial information, in particular where this use may be more susceptible to manipulation; and
 - (j) users lack the time, discipline or knowledge to effectively monitor the results of processing.
- .15 As the effectiveness of the design and operation of a CIS is dependent on systems development and logical access controls, the auditor would consider these factors during the risk assessment stage of the audit.
- .16 The design or operation of a CIS may introduce the potential for risks not present in similar manual systems. The auditor would consider the process by which computer information is produced, for example automatically generated sales invoices from a price matrix and the extent to which this affects audit risk.
- .17 As new CIS technologies emerge, they are frequently employed by entities to build increasingly complex computer systems that may include micro-to-mainframe links, distributed databases, end-user processing, and business management systems that feed information directly into the financial systems. Such technologies increase the overall sophistication of CIS's and the complexity of the specific applications that they affect. As a result, they may increase risk and require further consideration.
- .18 Increasingly, CIS's facilitate large volumes of information to be processed without review, based on pre-agreed rules, and reporting a small number of exceptions for manual follow-up. The design of the system therefore becomes increasingly important to ensure that errors are properly identified by the system. Further, where exceptions occur management needs to implement control procedures to ensure that the errors are properly investigated. In

AUS 214 "AUDITING IN A CIS ENVIRONMENT"

these circumstances, the auditor needs to consider, where appropriate, the effectiveness of the manual follow-up procedures implemented by management.

Audit Procedures

- .19 *In accordance with AUS 402 "Risk Assessments and Internal Controls", the auditor should consider the CIS environment in designing audit procedures to reduce audit risk to an acceptably low level.*
- .20 The application of audit procedures to gather audit evidence may be influenced by the methods of computer processing. The auditor can use either manual audit procedures, computer-assisted audit techniques, or a combination of both to obtain sufficient appropriate audit evidence. However, where an entity uses a computer for processing significant applications, it may be difficult or impossible for the auditor to obtain certain data for inspection, confirmation or inquiry without computer assistance.
- .21 The identification of the nature and operation of controls will affect audit risk and its components and therefore the nature, timing and extent of audit procedures. For example:
- (a) where there is a complex calculation, and inherent and/or control risks have been assessed as high due to, for instance the risk of error, the auditor may design audit procedures to obtain audit evidence regarding the quality of controls over changes to the CIS, and in particular the entity's testing of those changes. In addition, the auditor may amend the nature of planned substantive procedures by placing additional emphasis on analytical procedures or amend the extent of planned substantive procedures regarding the reperformance of calculations. Controls over logical access, while important, are of less significance in this instance; or
 - (b) where there are less complex calculations but inherent risk has been assessed as high due to, for instance, the increased risk of material misstatements in the financial report as a result of irregularities, the auditor may design audit procedures to obtain audit evidence regarding access to critical functions, particularly by users, and regarding controls which provide for effective review and approval.

AUS 214 "AUDITING IN A CIS ENVIRONMENT"

- .22 Because of the characteristics of a CIS environment, the nature, timing and extent of audit procedures may differ from those audit procedures conducted in a manual environment. For example:
- (a) the nature, timing and extent of audit procedures on the performance of computer controls and computer processes can be restricted to cover the key processes. These tests may be performed using, for example, test data. Their effectiveness is, however, subject to:
 - (i) conducting audit procedures which provide audit evidence as to the continuing and consistent operation of specific systems throughout the period;
 - (ii) obtaining an understanding regarding the various alternative processes which contribute to the process or control being tested and clearly defining these; and
 - (iii) assessing the effect of the key processes being affected by other processes or information; and
 - (b) the auditor may use the results of audit procedures conducted in prior periods when the auditor has obtained sufficient appropriate audit evidence that no changes to the CIS environment have been identified.
- .23 The nature of computer processing means that in evaluating the results of audit procedures, errors identified may have a significant effect, particularly where the errors relate to the logic of the application or standing data used by an application. In each instance, the auditor needs to understand the nature of the error identified and its effect, if any, on the nature, timing, extent and results of audit procedures.

Operative Date

- .24 This AUS is operative in relation to the first financial reporting period commencing on or after 1 July, 1996 and later reporting periods, although earlier application is encouraged. This AUS supersedes Statement of Auditing Practice AUP 4 "Auditing in an EDP Environment – General Principles" as issued in March 1984.

AUS 214 "AUDITING IN A CIS ENVIRONMENT"

Compatibility with International Standards on Auditing

- .25 The basic principles and essential procedures of this AUS and of International Standard on Auditing ISA 401, Auditing in a Computer Information Systems Environment, are consistent in all material respects.